UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

DIRECCIÓN DE POSGRADO

MAESTRÍA EN REDES Y TELECOMUNICACIONES

TEMA:

"SEGURIDAD INFORMÁTICA Y LA RELACIÓN EN LA UTILIZACIÓN DE INTERNET COMO HERRAMIENTA DE APOYO EN LA FORMACIÓN DE NIÑOS, NIÑAS Y ADOLESCENTES DE EDUCACIÓN INICIAL Y BÁSICA DEL CENTRO EDUCATIVO LA PRADERA"

Trabajo de Titulación

Previo a la obtención del Grado Académico de Magíster en Redes y Telecomunicaciones

Autor: Ing. Tannia Cecilia Mayorga Jácome

Tutor: Ing. Edgar Freddy Robalino Peña, Mg.

Ambato – Ecuador

2014

Al Consejo de Posgrado de la Universidad Técnica de Ambato.

El Tribunal de Defensa del trabajo de titulación presidido por Ing. Edison Homero Álvarez Mayorga, Mg., Presidente del Tribunal e integrado por los señores Ingeniero Edwin Hernando Buenaño Valencia, Mg., Ing. Clay Fernando Aldás Flores, Mg., Ing. Teresa Milena Freire Aillón, Mg., Miembros del Tribunal de Defensa, designados por el Consejo Académico de Posgrado de la Facultad de Ingeniería en Sistemas Electrónica e Industrial de la Universidad Técnica de Ambato, para receptar la defensa oral del trabajo de titulación para graduación con el tema: "SEGURIDAD INFORMÁTICA Y LA RELACIÓN EN LA UTILIZACIÓN DE INTERNET COMO HERRAMIENTA DE APOYO EN LA FORMACIÓN DE NIÑOS, NIÑAS Y ADOLESCENTES DE EDUCACIÓN INICIAL Y BÁSICA DEL CENTRO EDUCATIVO LA PRADERA", elaborado y presentado por la señora Ing. Tannia Cecilia Mayorga Jácome, para optar por el Grado Académico de Magister en Redes y Telecomunicaciones.

Una vez escuchada la defensa oral el Tribunal aprueba y remite el trabajo de titulación para uso y custodia en las bibliotecas de la UTA.

Ing. Edison Homero Álvarez Mayorga, Mg.

Ing. Teresa Milena Freire Aillón, Mg.

Ing. Edwin Hernando Buenaño Valencia, Mg.

Ing. Clay Fernando Aldás Flores, Mg.

AUTORÍA DE LA INVESTIGACIÓN

La responsabilidad de las opiniones, comentarios y críticas emitidas en el trabajo de titulación con el tema: "SEGURIDAD INFORMÁTICA Y LA RELACIÓN EN LA UTILIZACIÓN DE INTERNET COMO HERRAMIENTA DE APOYO EN LA FORMACIÓN DE NIÑOS, NIÑAS Y ADOLESCENTES DE EDUCACIÓN INICIAL Y BÁSICA DEL CENTRO EDUCATIVO LA PRADERA", le corresponde exclusivamente a: Ing. Tannia Cecilia Mayorga Jácome, Autor bajo la Dirección de Ing. Edgar Freddy Robalino Peña, Mg., Director del trabajo de titulación; y el patrimonio intelectual a la Universidad Técnica de Ambato.

---	---
Ing. Tannia Cecilia Mayorga Jácome	Ing. Edgar Freddy Robalino Peña, Mg.
Autor	Director

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga uso de este trabajo de titulación como un documento disponible para su lectura, consulta y procesos de investigación.

Cedo los Derechos de mi trabajo de titulación, con fines de difusión pública, además autoriza su reproducción dentro de las regulaciones de la Universidad.

Ing. Tannia Cecilia Mayorga Jácome

C.C. 1711228997

DEDICATORIA

Por toda la paciencia y tiempo que tuvieron que verse privados de mi compañía dedico esta tesis a los varones más importantes de mi vida: mi esposo, a mi hijo, a mi Padre.

Nombre(s)

Ing. Henry Rodrigo Vivanco Herrera

José Daniel Vivanco Mayorga

Lic. José Alfredo Mayorga Ballesteros

AGRADECIMIENTO

A mi Director de Tesis Ing. Freddy Robalino Mg. por su paciencia, sus conocimientos valiosos y todo el tiempo que dedicó en las reuniones para dirigir esta tesis.

A Ing. Mauricio Quisimalín Msc. quien me encaminó durante la elaboración del Plan de Tesis.

Arq. Luis Atapuma Propietario del Centro Educativo La Pradera quien autorizó el desarrollo de esta Tesis en su Institución con miras a mejorar la seguridad de los estudiantes.

Personal Administrativo y Docente del Centro Educativo La Pradera por colaborar durante el proceso investigativo para las mediciones, encuestas, reuniones.

Estudiantes del Centro Educativo La Pradera por colaborar en forma desinteresada y sincera para esta investigación que ayudará a que tengan seguridad informática durante su formación.

Padres de familia del Centro Educativo La Pradera por contestar las encuestas enviadas.

ÍNDICE GENERAL

PÁGINAS PRELIMINARES

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

ÍNDICE DE DOCUMENTOS

ÍNDICE DE FÓRMULAS

UNIVERSIDAD TÉCNICA DE AMBATO
FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL
DIRECCIÓN DE POSGRADO
MAESTRÍA EN REDES Y TELECOMUNICACIONES

Tema "SEGURIDAD INFORMÁTICA Y LA RELACIÓN EN LA UTILIZACIÓN DE INTERNET COMO HERRAMIENTA DE APOYO EN LA FORMACIÓN DE NIÑOS, NIÑAS Y ADOLESCENTES DE EDUCACIÓN INICIAL Y BÁSICA DEL CENTRO EDUCATIVO LA PRADERA"

Autor: Ing. Tannia Cecilia Mayorga Jácome
Director: Ing. Edgar Freddy Robalino Peña, Mg.
Fecha: 27 de noviembre de 2013

RESUMEN EJECUTIVO

La investigación sobre Seguridad Informática y la relación en la utilización de internet como herramienta de apoyo en la formación de niños, niñas y adolescentes de educación inicial y básica del Centro Educativo La Pradera tiene como objetivo general determinar la seguridad informática y la relación en la utilización de Internet como herramienta de apoyo en la formación de niños, niñas y adolescentes. Luego de hacer un estudio de análisis de riesgos usando la norma ISO 27005:2008, se presenta una propuesta que permita mejorar la seguridad informática y los problemas asociados a esta, proponiendo un rediseño de la red usando una estructura jerárquica y un Plan de seguridad informático usando la norma ISO 27001:2005 en lo referente a Planear, de esta forma los docentes podrán hacer uso de la infraestructura tecnológica de una manera segura para formar a los estudiantes, y los estudiantes podrán hacer uso de la misma reduciendo los riesgos existentes en Internet. La norma ISO 27001 involucra a toda la organización: Procesos de negocio, Personas, Hardware, Software, Red, Medios y sobre todo entrega la responsabilidad del seguimiento de la seguridad de la información a los propietarios, directores, jefaturas. Al ser integral la seguridad

de la información, conocida también como seguridad informática se presenta también una propuesta de un Plan de capacitación del uso de Herramientas como Webquest y Cazas de Tesoros en calidad de herramientas de búsquedas guiadas, ya que se evidencia un desconocimiento total por parte de los docentes del uso de las mismas; y a los padres de familia un Taller de ventajas, riesgos sobre el uso de Internet y soluciones tecnológicas para disminuir el riesgo de las amenazas existentes en Internet.

Descriptores: Análisis de riesgos, formación de niños, niñas y adolescentes, Internet en el aula, Norma ISO 27001, Norma ISO 27005, plan de seguridad informática, plan de capacitación uso de webquest, plan taller para padres de familia sobre seguridad informática, red jerárquica, seguridad informática, ventajas y riesgos niños, niñas y adolescentes con el uso de Internet.

UNIVERSIDAD TÉCNICA DE AMBATO
FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL
DIRECCIÓN DE POSGRADO
MAESTRÍA EN REDES Y TELECOMUNICACIONES

Theme "COMPUTER SECURITY RELATIONSHIP AND USE OF INTERNET AS A TOOL FOR TRAINING SUPPORT CHILD AND ADOLESCENT EDUCATION AND INITIAL BASIC EDUCATION CENTER " LA PRADERA""

Author: Ing. Mayorga Jácome Tannia Cecilia
Directed by: Ing. Edgar Freddy Robalino Peña, Mg.
Date: November, 27th 2013

EXECUTIVE SUMMARY

Research on Information Security and the relationship in the use of internet as a support tool in the education of children and adolescents of initial and basic Education School La Pradera general objective of information security and determine the relationship between Internet use as a support tool in the education of children and adolescents. After a study of risk analysis using the ISO 27005 standard, a proposal to improve computer security and the problems associated with this, proposing a redesign of the network using a hierarchical structure and a Plan of computer security is presented using the ISO 27001 regarding Planning, thus teachers can make use of the technological infrastructure of a safe way to train students, and students may use the same reducing the risks on the Internet. The ISO 27001 standard involves the entire organization: Business Processes, People, Hardware, Software, Network, Media and especially the responsibility for monitoring delivery of information security to the owners, directors, and headquarters. As the comprehensive information security, computer security also known as a proposed training plan using tools like Webquest and Treasure Hunts

as guided search tools is also presented, as is a total lack of evidence for part of teachers in the use thereof, and Parent Training about advantages, risks and the use of Internet technology to reduce the risk of threats in Internet solutions.

Keywords: benefits and risks of children and adolescents with Internet use, hierarchical network, Internet in the classroom, ISO 27001, ISO 27005, information security plan, information security, plan workshop for parents on computer security, risk analysis, training of children and adolescents, training plan using webquest,.

INTRODUCCIÓN

La seguridad informática en los Centros Educativos es un tema que requiere de especial atención por el avance tecnológico que se viene dando a pasos agigantados y junto a ello el uso de las Tecnologías de Información y Comunicación (TIC), adicional es la curiosidad de niños, niñas y adolescentes en calidad de nativos tecnológicos que muchas veces no tienen la madurez psicológica para enfrentar la inmensa cantidad de información disponible abiertamente en el Internet y se encuentran expuestos a peligros.

El riesgo es que un Docente al usar el Internet como material de apoyo en TICs, este se tope que el estudiante accedió a un lugar diferente del indicado, lo cual genera distracción en el estudiante y en el docente al solicitar al estudiante que se centre en lo indicado.

Si bien es cierto no existe un Sistema de Seguridad 100% seguro, es necesario que se definan políticas, normas, aplicación de estándares, responsabilidades para precautelar con la seguridad de la niñez y adolescencia.

Es por esto que el presente tema de investigación tiene como importancia fundamental diagnosticar y proponer políticas de seguridad para el Centro Educativo La Pradera como medida de protección de los estudiantes que día a día acuden a formarse.

CAPÍTULO I

EL PROBLEMA

1.1 Tema de Investigación

"SEGURIDAD INFORMÁTICA Y LA RELACIÓN EN LA UTILIZACIÓN DE INTERNET COMO HERRAMIENTA DE APOYO EN LA FORMACIÓN DE NIÑOS, NIÑAS Y ADOLESCENTES DE EDUCACIÓN INICIAL Y BÁSICA DEL CENTRO EDUCATIVO LA PRADERA"

1.2 Planteamiento del problema

1.2.1 Contextualización

1.2.1.1 **Macro**

En España el documento publicado por Josep Pujadas i Jubany el 3 de julio del año 2008 sobre la Seguridad Informática en los Centros Educativos de Valladolid cuya conclusión es "no hay un modelo seguro y que hay que adaptarlo a las necesidades de cada Institución".

1.2.1.2 **Meso**

En Panamá el Ministerio de Educación está aplicando un modelo CRA cuyo objetivo principal es "coadyuvar al logro de una Educación Moderna y de Calidad, en un Marco Democrático y Equitativo" a Centros Educativos que se enfoca a: Modelo de laboratorios, reglas de uso aplicadas, lineamientos, adquisiciones.

1.2.1.3 **Micro**

En Ecuador en el año 2011 se realiza la tesis en la Universidad Israel extensión Cuenca, con el tema "Estudio, propuesta y aplicación de políticas de seguridad en los laboratorios de informática" para las entidades educativas: Enriqueta Cordero Dávila, y Remigio Crespo Toral, cuya conclusión dice que "La navegación en el internet se ha vuelto una actividad diaria por parte de los estudiantes ellos acceden a la red para investigar, chatear, observar videos establecer vínculos en redes sociales. Razón por eso es importante un nivel de seguridad en la red, en donde posibilite tomar ciertas decisiones que restrinjan ciertas páginas con contenido inadecuado para una formación pedagógica, que demanda la educación básica."

En general se puede decir que Ecuador tiene una gran debilidad en lo que se refiere a Seguridad Informática en los Centros Educativos de Educación Inicial y Básica, y no existe un modelo general de políticas de seguridades informáticas a aplicarse en los Centros Educativos de Educación Inicial y Básica dejando mucho espacio para que los niños, niñas y adolescentes estén expuestos a los peligros informáticos.

Los padres de familia de los niños(as) de Educación inicial, permiten que sus hijos(as) manejen software de celulares como juegos o videos musicales lo que hace que desde edades muy cortas usen la tecnología a la perfección y la curiosidad les lleva a indagar en opciones que muchas veces un adulto no lo haría.

En Educación básica ya existen estudiantes que usan computadores portátiles, notebooks o tecnología móvil sin seguridad alguna, incurriendo en muchos riesgos.

Se hace necesario aplicar normas para respaldar las políticas a ser implementadas, definir roles, responsabilidades para que cada quien asuma su responsabilidad.

1.2.2 Árbol de Problemas

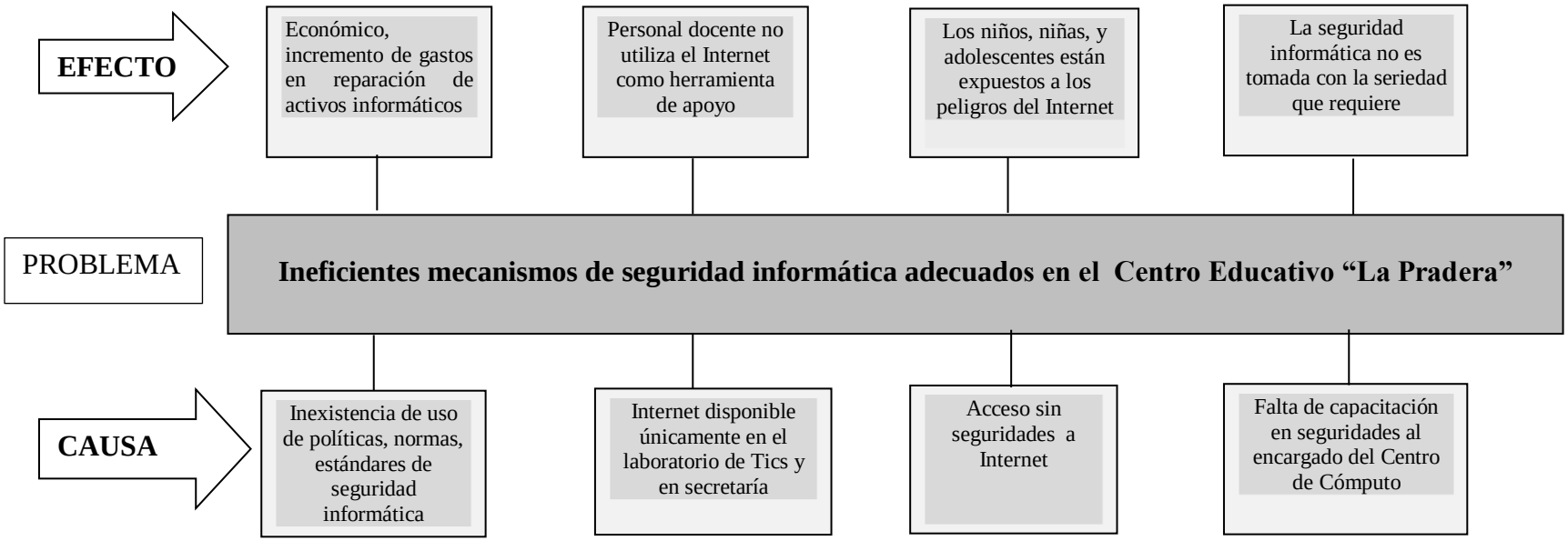


Gráfico: 1.1 Árbol del Problema (Elaborado por: Investigador)

1.2.3 Análisis crítico

Los ineficientes mecanismos de seguridad informática en el Centro Educativo La Pradera, ha tenido efectos en el ámbito económico ya que se han incrementado los gastos en reparación de activos informáticos por la inexistencia de políticas, normas, procedimientos, uso de estándares de seguridad informática.

El hecho de que el Internet esté disponible únicamente en el Laboratorio de Tics y en secretaría, restringe la posibilidad de que el Personal Docente utilice el Internet como herramienta de apoyo, para investigación o preparar el material para sus clases.

Hoy en día el uso de las Tecnologías de la Información en los niños, niñas y adolescentes está en boga y es algo inevitable ya que ellos son nativos tecnológicos; la curiosidad y el deseo de hacer cosas que hacen los adultos y divertirse hace que busquen cosas y se encuentren expuestos a peligros como pornografía, redes de tráfico de menores, engaños entre otros.

Muchas veces se enfrentan a información visual que no están preparados para asimilar psicológicamente y tampoco se atreven a preguntar a un adulto o no tienen a un adulto cerca, ocasionando una mala interpretación propia o de otro menor.

La Era Contemporánea conocida como la era de la Incertidumbre porque la Tecnología avanza a pasos agigantados, obliga a los Docentes a capacitarse en su uso como medio didáctico para impartir clases en el aula, en donde el Docente ya no es el dueño del conocimiento, sino que es una guía para ayudar a que el estudiante “aprenda a aprender”; actualmente se observa que un estudiante se aburre en clases porque en casa maneja tecnología que le atrae, que le interesa mientras que en el aula muchos Docentes continúan sus clases con técnicas de hace veinte años.

De ahí la necesidad de que el docente use el Internet como medio o herramienta de apoyo en el aula para impartir sus clases, pero de una manera segura para que sea algo productivo, para que el estudiante aprenda a aprender organizadamente, sin salirse de las indicaciones dadas por los maestros(as) y con las seguridades adecuadas.

El laboratorio de Tics no tiene seguridades en el control de acceso a Internet por lo que los niños, niñas y adolescentes se encuentran expuestos a los peligros del Internet.

Por otra parte tener tecnología no es únicamente adquirirla y ubicarla en un espacio, en el caso de entidades educativas o de otra índole requiere de una organización informática de aplicar políticas, normas de seguridad, establecer roles, responsabilidades, funcionar bajo estándares con miras hacia la calidad y excelencia no únicamente para protección de la información, del patrimonio o de la economía sino para garantizar una educación íntegra del Patrimonio más valioso que constituye el elemento humano que tiene a cargo en la formación de niños, niñas y adolescentes.

1.2.4 Prognosis

De mantenerse el problema de ineficientes mecanismos de seguridad informática adecuados en el Centro Educativo La Pradera a futuro se tendrá que los niños, niñas y adolescentes accedan sin problema a pornografía, páginas no aptas, se enfrenten a peligros como redes de tráfico de menores, engaños, cyberbulling, sexting, acoso, entre otros; baje el prestigio de la Institución por la mala reputación tecnológica, trayendo como consecuencia la disminución alumnos matriculados por la desconfianza generada; y a su vez causando un desequilibrio económico en la misma.

La curiosidad, la intencionalidad de divertirse de los niños, niñas y adolescentes lleva a experimentar con los medios tecnológicos de cualquier índole y sus consecuencias hace que aprendan día a día de esas experiencias pero ese aprendizaje puede constituirse en una amenaza si no se tienen definido políticas, normas, procedimientos, definidos roles y

responsabilidades para precautelar con la integridad de los bienes tecnológicos de una entidad Educativa conllevando muchas veces a incurrir en gastos no presupuestados para mantener un laboratorio de informática en óptimas condiciones.

Los docentes no podrán estar actualizados en las herramientas como Internet, ya que en la Institución no pueden hacer uso de esta para preparar sus clases en las horas pedagógicas, o quizá usar el Internet como material de apoyo, o investigación, cuya consecuencia sería grave ya que los estudiantes estarían más actualizados que los Docentes ya que estos son nativos tecnológicos.

1.2.5 Formulación del problema

¿Cómo incide la seguridad informática en la utilización de Internet como herramienta de apoyo en la formación de niños, niñas y adolescentes de Educación Inicial y Básica del Centro Educativo La Pradera?

1.2.5.1 Interrogantes de Investigación

¿Existen políticas, normas, procedimientos, estándares de seguridad informática para la utilización de internet como herramienta de apoyo en el Centro Educativo La Pradera?

¿Qué tipo de educación permite el internet como herramienta de apoyo en la formación de los niños, niñas y adolescentes del Centro Educativo La Pradera.?

¿Cuáles serían las políticas, normas, procedimientos o estándares de seguridad informática para la utilización de internet como herramienta de apoyo que permita mejorar la formación de niños, niñas y adolescentes de Educación Inicial y Básica del Centro Educativo La Pradera.?

1.2.5.2 **Delimitación de la investigación**

Campo: Seguridad Informática

Área: Informática

Aspecto: Internet como herramienta de apoyo en la formación.

Espacial: la Investigación se realizará en el Centro Educativo La Pradera de Sangolquí, cantón Rumiñahui, provincia de Pichincha para educación Inicial 2 y Educación Básica.

Temporal: La investigación se llevará a cabo en el período comprendido entre mayo y noviembre del 2013.

1.3 Justificación

El área educativa, concretamente la formación de estudiantes de educación básica es un tema que va de la mano con el uso de Internet por parte de los profesores para estar acorde al avance tecnológico que los niños, niñas y adolescentes manejan a la perfección. Actualmente la seguridad informática es un tema que es muy nombrado pero poco aplicado, muchas veces cuando sucede algo grave es cuando las entidades de cualquier índole empiezan a tomar medidas correctivas.

Tanto en instituciones educativas de carácter fiscal como particular no existen partidas presupuestarias para el responsable de TI, dicho rol en lo que le queda de tiempo, lo asume el profesor de computación ya que el resto del tiempo debe dedicarse a la cátedra asignada, es por ello que esta investigación será de utilidad para que se aplique el Plan de seguridad informática en pro de mejorar la seguridad informática de la institución ayudando tanto a docentes como a estudiantes a tener un ambiente tecnológico seguro, a la vez que

concientizar a los Propietarios, autoridades de que es responsabilidad de ellos en primera instancia velar para que se cumpla y no queden expuestos los estudiantes a los peligros del Internet.

El uso de Internet sin restricciones en la Educación básica se viene convirtiendo en un tema importante ya que muchas veces los estudiantes no tienen la madurez psicológica para asimilar la información abierta o se encuentran expuestos a peligros informáticos como la pornografía, redes de trata de menores, fraudes informáticos, engaños etc.

Al tener libre acceso, la curiosidad de los estudiantes conlleva a ingresar a páginas web diferentes a las indicadas en clases causando falta de atención a las indicaciones de los maestros.

Cuando se habla de grandes empresas, se menciona activos, información, en este caso los seres humanos vienen a constituir algo mucho más valioso que cualquier activo del mundo ya que los niños, niñas y adolescentes son el futuro de nuestra Patria.

La investigación es factible ya que se cuenta con el apoyo de los propietarios del Centro Educativo La Pradera.

1.4 Objetivos

1.4.1 General

Determinar cómo incide la seguridad informática en la utilización de Internet como herramienta de apoyo en la formación de niños, niñas y adolescentes de Educación Inicial y Básica del Centro Educativo La Pradera.

1.4.2 Específicos

Indagar sobre la existencia de políticas, normas, procedimientos o estándares de seguridad informática para la utilización de internet como herramienta de apoyo en el Centro Educativo La Pradera.

Identificar qué tipo de formación permite el internet como herramienta de apoyo en los niños, niñas y adolescentes del Centro Educativo La Pradera.

Definir cuáles serían las políticas, normas, procedimientos o estándares de seguridad informática para la utilización de internet como herramienta de apoyo que permita mejorar la formación de niños, niñas y adolescentes de Educación Inicial y Básica del Centro Educativo La Pradera.

CAPÍTULO II

MARCO TEÓRICO

2.1 Antecedentes de investigación

En el desarrollo de la presente investigación se ha considerado determinar cómo incide y la seguridad informática en la utilización de Internet como herramienta de apoyo en la formación de niños, niñas y adolescentes de Educación Inicial y Básica del Centro Educativo La Pradera CELP elaborando un Plan de Seguridad Informática.

En Argentina en el gobierno de la Presidenta Cristina Fernández de Kirchner , ICIC el Programa nacional de infraestructuras críticas de información y ciberseguridad, publica un documento Titulado "Navegación Segura y uso responsable de Internet" uno de los párrafos que llama la atención es: "Resulta vital, entonces, conocer los riesgos a los cuales se exponen los niños, niñas y adolescentes con el objeto de tomar conciencia, estar prevenidos, protegerlos de cualquier posible daño y enseñarles el "buen uso" de las tecnologías" (Gobierno de Argentina, 2009, pág. 3) en donde presenta una lista de riesgos a los que se exponen los niñas, niños y adolescentes ante el uso de internet como son:

- Violación a la intimidad
- Robo o suplantación de identidad
- Abuso emocional
- Abuso sexual i/o violencia

- Exposición a material inadecuado o engañoso
- Acoso entre pares usando las nuevas Tecnologías de la Información y Comunicación (TIC) o "cyberbulling"
- Infracción a leyes, normas o disposiciones (Gobierno de Argentina, 2009, págs. 2-5)

En Valladolid, el autor Pujadas i Jubany en el año 2008 presenta un proyecto de seguridad en redes para Centros Educativos, en el que presenta una propuesta segura a nivel de diseño de red aplicable a Centros Educativos en general.

El autor Rubén Darío Campusano Rodríguez desarrolló un estudio en el área educativa como es el siguiente "Estudio, propuesta y aplicación de políticas de seguridad en los laboratorios de informática en las instituciones educativas de nivel básico" para un laboratorio que no tenga servidor de dominio (Campusano Rodríguez, 2011) , en donde enfoca las preferencias de accesos a Internet de niños y jóvenes en la ciudad de Cuenca; vulnerabilidades de un laboratorio a nivel físico, Filtros de contenido, Servidores de Seguridad, Servidores de firewall.

2.2 Fundamentación filosófica

La presente investigación la realizaré utilizando el paradigma **crítico propositivo**; critico porque se señala claramente la falta de aplicabilidad de políticas de seguridad informática en los Centros Educativos de Educación Inicial y Básica, con sus efectos muy serios que este problema genera; y propositivo por cuanto busca plantear una propuesta de seguridad informática.

2.3 Fundamentación sociológica

El trabajo de investigación se sustenta en la necesidad del área educativa de evolucionar al cambio tecnológico, pero considerando las seguridades que se requieren para hacerlo de una manera responsable ya que está en juego la formación de niños, niñas y adolescentes.

2.4 Fundamentación legal

La presente investigación se fundamenta en la Ley Orgánica de Educación Intercultural LOEI, capítulo IV, sección III, Art. 53 en Funciones del Consejo Ejecutivo en el numeral 5, dice "Diseñar e implementar estrategias para la protección integral de los estudiantes;" (LOEI, 2011, pág. 18) y en el capítulo VIII, art. 342 numeral 4 menciona "realizar el seguimiento en el ámbito educativo del cumplimiento de las medidas de protección dictadas por las autoridades competentes en la protección de los estudiantes".

2.5 Categorías fundamentales

2.5.1 Organizador lógico de variables

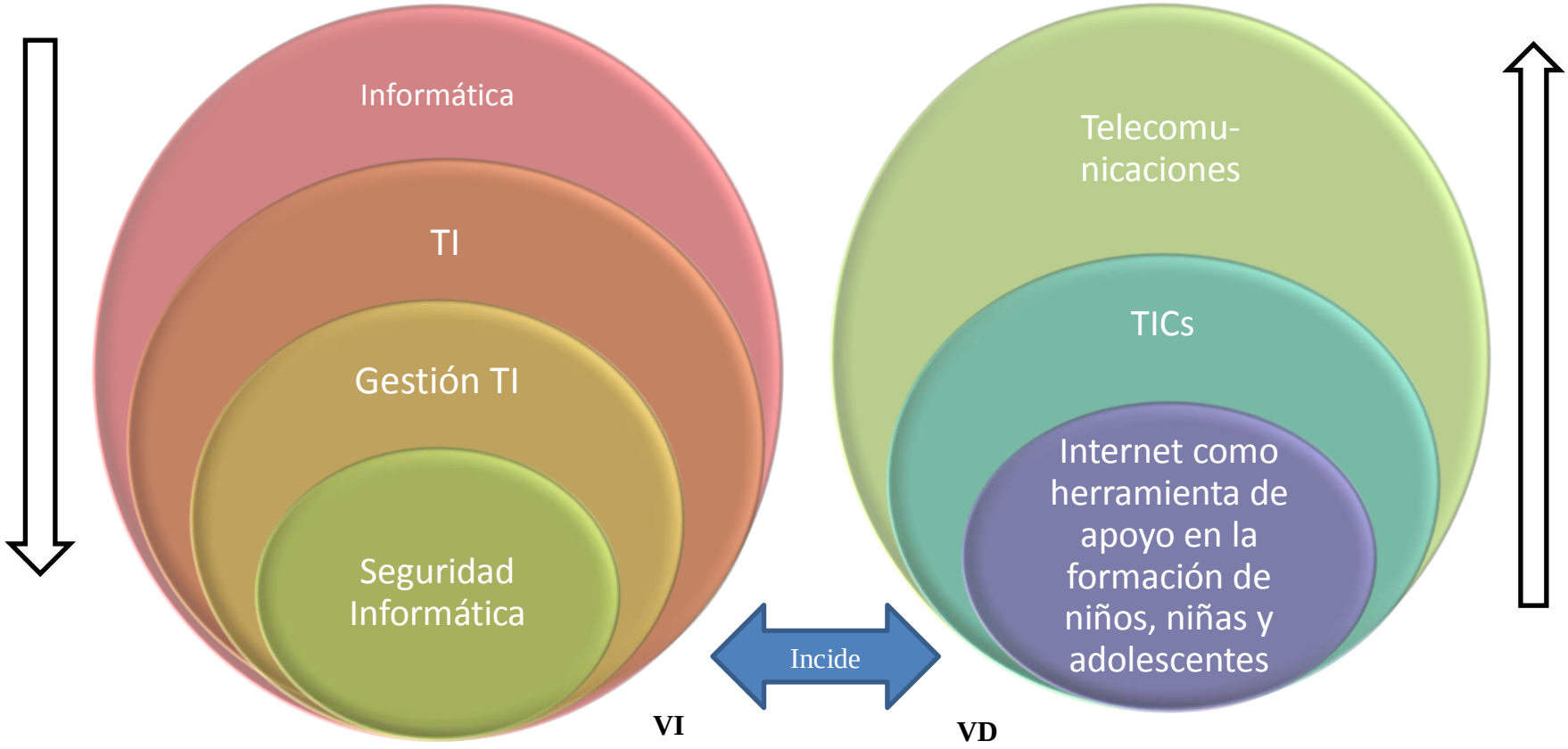


Gráfico: 2.1 Categorías Fundamentales (Elaborado por: Investigador)

2.5.2 Constelación de Ideas, Mandala Variable Independiente u otros

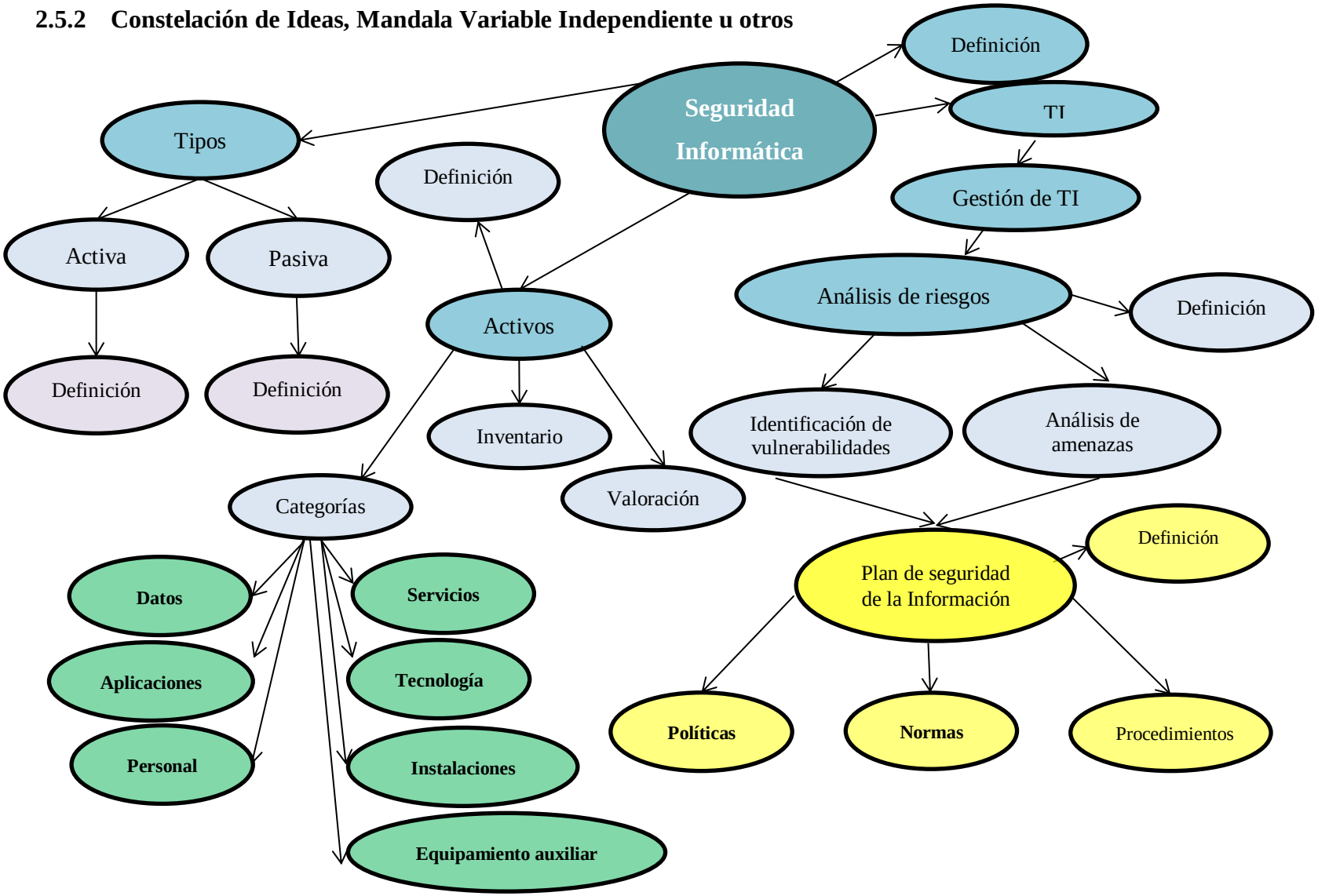


Gráfico:.2.2 Constelación de Ideas Variable Independiente (Elaborado por: Investigador)

2.5.3 Constelación de Ideas, Mandala Variable Dependiente u otros

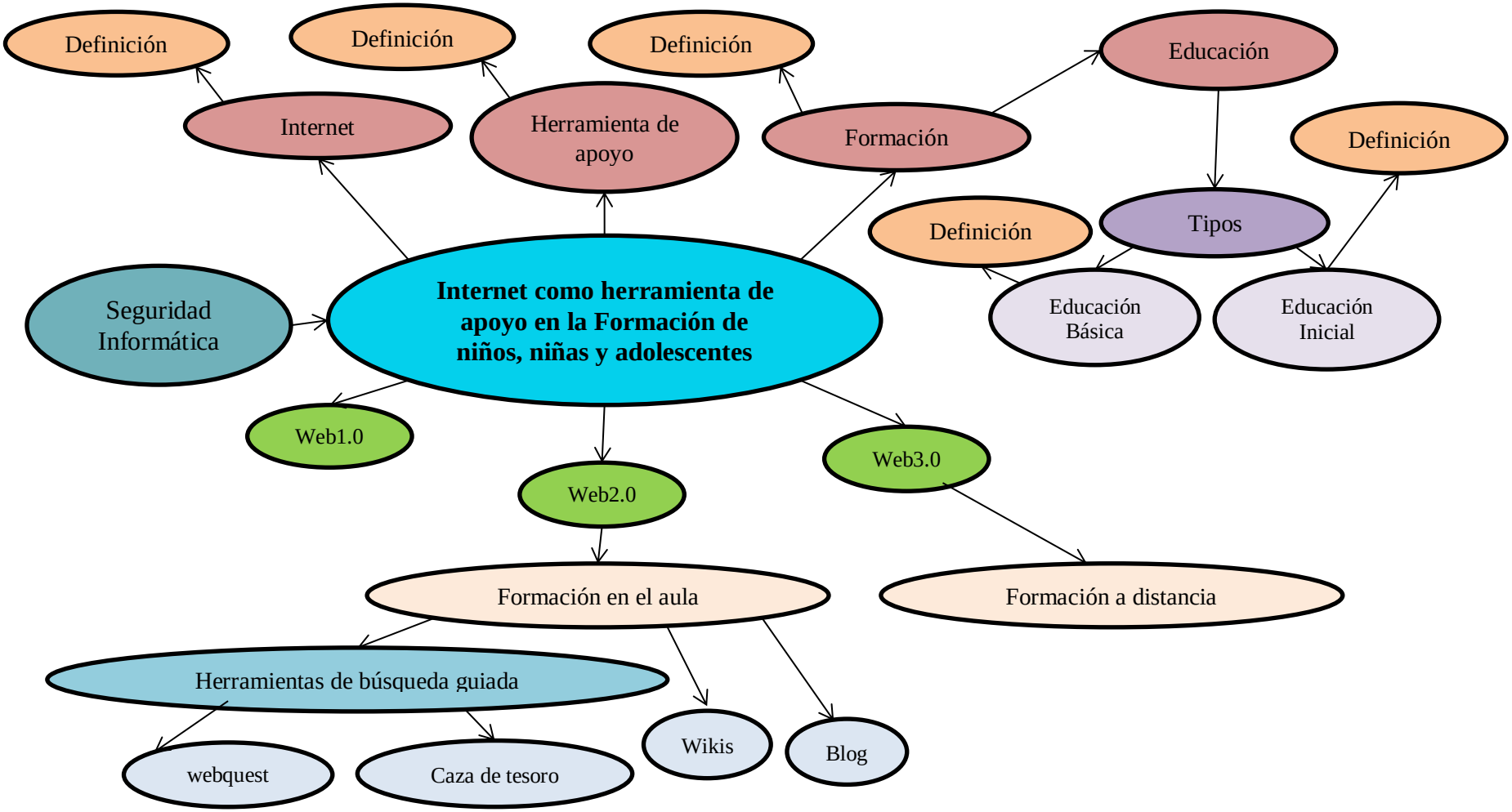


Gráfico: 2.3 Constelación de Ideas Variable Dependiente (Elaborado por: Investigador)

2.5.4 Categorías de la variable Independiente

2.5.4.1 **Informática**

"Conjunto de técnicas en que se basan los procesos de tratamiento automático de la información mediante computadoras u operadores electrónicos." (Departamento de obras de referencia Ediciones Trébol,S.L., 2007, pág. 498). La Informática en general es una ciencia creativa formada por técnicas, procesos, estándares, métodos, entre otros, que permiten estar en constante automatización y es aplicable a todas las áreas como por ejemplo la informática centrada en la red y la informática orientada a la educación.

"Informática centrada en la red (network-centric computing) s. Un entorno informático en el que uno o más servidores de red representan el centro de actividad. Considerado como la "tercera ola" en la informática de grandes sistemas, después del desarrollo de los mainframe y de los equipos de escritorio, la informática centrada en la red establece a los servidores como fuente principal de potencia de procesamiento con el fin de dar a los usuarios acceso directo a información y aplicaciones basadas en la red. En los sistemas informáticos centrados en la red, las aplicaciones no están preinstaladas ni se tienen que desinstalar localmente, es decir, en el equipo de escritorio; en lugar de ello, se accede a las aplicaciones según va siendo necesario, "sobre la marcha". De esa forma, los equipos de escritorio individuales no tienen por qué disponer de grandes cantidades de espacio de almacenamiento en disco ni tampoco tiene por qué cargar ni gestionar programas de aplicación." (Vuelapluma, S., 2003, págs. 173-174) .

La informática vista desde el área educativa requiere la integración de las Tecnologías de información con comunicaciones y necesita ser gestionada de tal forma que tanto los docentes y estudiantes puedan aprovechar de la tecnología de una manera eficiente y segura durante la formación o al utilizarla como herramienta de apoyo en el aula.

2.5.4.2 **Gestión TI**

"Gestión de TI es todo lo relativo a la adquisición, tratamiento, almacenamiento y diseminación de la información en todas sus formas (textual, numérica, gráfica, pictórica, vocal) con la ayuda de computadoras y sistemas de telecomunicación." (Clayton, 2002).

Existen varios estándares que permiten gestionar TI como son la ISO 20000 (desarrollo a nivel táctico), Cobit (Objetivos de Control para Tecnología de Información y Tecnologías relacionadas), Itil (regular la prestación de servicios de TI).

La gestión de TI consiste en tomar decisiones referentes a TI sobre aspectos operativos para suministrar productos y servicios en forma eficaz permite garantizar que toda la información y los procesos relacionados a esta se encuentren trabajando en óptimas condiciones tratando siempre de identificar riesgos para realizar el tratamiento adecuado y que el proceso de negocio de la institución en la cual se aplica funcione adecuadamente.

Todo esto implica tener al frente una persona que se encargue de gestionar la seguridad, la misma que esté siempre evaluando riesgos y sobre todo que tenga el apoyo de la gerencia, jefaturas, ya que la responsabilidad de la seguridad es de todos pero principalmente de la gerencia.

2.5.4.3 **TI**

"Conocido como IT son las siglas de tecnología de información " (Clayton, 2002, pág. 414).

"Tecnología de la información (information technology) Estudios realizados para mejorar el procesamiento de datos y la información mediante el uso de máquinas y dispositivos cada vez más avanzados." (Clayton, 2002, pág. 406).

En el área educativa las Tecnologías de información y comunicación cada vez cobran mayor importancia debido a que los docentes empiezan a utilizar las TICs en el aula como recurso pedagógico que ayuda a aplicar el constructivismo fomentando la reflexión, en los estudiantes.

Desafortunadamente el área de TI aun no es tomado en cuenta como se debería en el ámbito educativo pues no existe una partida presupuestaria para un responsable de esta área en el sector público, y en el sector privado aún no han asimilado la mayoría de propietarios la importancia que conlleva tener un departamento de TI que se encargue de gestionar la seguridad de la información.

2.5.4.4 **Seguridad Informática**

2.5.4.4.1 Definición

La seguridad informática, es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con ésta (incluyendo la información contenida) y puede ser aplicada en cualquier ámbito como es la educación, en donde juega un papel fundamental la aplicación de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos en el área tecnológica, ya sea de laboratorios de computación, de equipos que maneja el personal administrativo y docente, la infraestructura de red, información y sistemas con sus respectivas bases de datos que se utilicen para facilitar la gestión de matrículas, calificaciones, entre otros; es decir constituye todo lo que la organización valore como activo y signifique un riesgo si esta llega a manos de otras personas. (Matilla, A., 2013, pág. 1)

A continuación citaré definiciones textuales de seguridad informática:

"La seguridad informática es una disciplina que se relaciona con diversas técnicas, aplicaciones y dispositivos encargados de asegurar la integridad y privacidad de la información de un sistema informático y sus usuarios." (Alegsa, 2012).

“La Seguridad informática está basada en las Tecnologías de Información, las comunicaciones TIC, se basa en el manejo de vulnerabilidades, amenazas bajo la forma de ataques, valuación de activos” (Omerella, M., pág. 1).

2.5.4.4.2 Tipos de Seguridad

- Activa
- Pasiva

Seguridad Activa

Son las medidas que se utilizan para detectar las amenazas, y después de ello evitar, o reducir los riesgos. (García, Huratado, & Alegre Ramos, Seguridad informática, 2011).

Seguridad Pasiva

“Son las medidas que se implantan para, una vez producido el incidente de seguridad, minimizar su repercusión y facilitar la recuperación de los datos” (Castells, M., 2010).

Mecanismos de Seguridad

Se considera a todo aquello de naturaleza hardware como software que se utilice para crear reforzar y mantener la seguridad informática.

El Autor (Pujadas I Jubany, 2008). Señala. “La conclusión es que la seguridad al cien por cien no existe, pero tenemos que pensar en cuál es la estructura más segura que podemos permitirnos”; a esta conclusión puedo añadir que la estructura más segura depende del entorno en el que se vaya a aplicar.

2.5.4.4.3 Seguridad de la Información

Information security o Seguridad de la Información es la traducción más adecuada que se le viene dando a lo que no involucra únicamente el puro enfoque técnico sino abarca algo más amplio que lo técnico pues implica responsabilidades de alta gerencia y cuadros directivos de una organización. (Omerella, M., pág. 1), tomando en consideración que el ambiente Tic tiende a estar orientado al servicio y a actuar como función habilitante de los procesos de negocios de una empresa.

Es primordial el involucramiento activo de los líderes de las organizaciones, que para el área educativa constituyen: Propietarios, Rector, Vicerrector, Inspector entre otros para crear un plan sustentable de seguridad de la información a partir de los riesgos determinados; actualmente se considera la gente, los procesos, funciones de negocio, protección de los recursos o activos de la organización donde toda la empresa es la impulsora y beneficiaria de la seguridad de la información en un marco de responsabilidades compartidas. (Omerella, M., págs. 1,2).

Por tanto no se consideran únicamente los riesgos técnicos sino también los riesgos de seguridad que se extiende a toda la empresa, es decir: organizacionales, operacionales, físicos. (Omerella, M., págs. 1,2).

2.5.4.4.4 Valuación de Activos

Activo

"Activo es cualquier cosa que tenga valor para la organización" (ISO/IEC, 13335-1:2004)

"Activos de información son ficheros y bases de datos, contratos y acuerdos, documentación del sistema, manuales de los usuarios, material de formación, aplicaciones, software del sistema, equipos informáticos, equipo de comunicaciones, servicios informáticos y de comunicaciones, utilidades generales como por ejemplo calefacción,

iluminación, energía y aire acondicionado y las personas, que son al fin y al cabo las que en última instancia generan, transmiten y destruyen información, es decir dentro de un organización se han de considerar todos los tipos de activos de información" (Poveda, J.M., 2011).

Categorías

Categoría	Descripción
Datos	Todos aquellos datos que se generan, recogen, gestionan, transmiten y destruyen en la organización.
Aplicaciones	El software que se utiliza para la gestión de la información.
Personal	En esta categoría se encuentra tanto la plantilla propia de la organización, como el personal subcontratado, los clientes, usuarios y, en general, todos aquellos que tengan acceso de una manera u otra a los activos de información de la organización.
Servicios	Se consideran tanto los servicios internos, aquellos que una parte de la organización suministra a otra (por ejemplo la gestión administrativa), como los externos, aquellos que la organización suministra a clientes y usuarios (por ejemplo la comercialización de productos).
Tecnología	Los equipos utilizados para gestionar la información y las comunicaciones (servidores, PCs, teléfonos, impresoras, routers, cableado, entre otros)
Instalaciones	Lugares en los que se alojan los sistemas de información (oficinas, edificios, vehículos, entre otros.)
Equipamiento auxiliar	En este tipo entrarían a formar parte todos aquellos activos que dan soporte a los sistemas de información y que no se hallan en ninguno de los tipos anteriormente definidos (equipos de destrucción de datos, equipos de climatización, entre otros.)

Tabla 2.1 Ejemplos de categorías de los Activos (Fuente: Poveda, J.M., 2011, págs. 1-2)

Inventario de Activos

Con la finalidad de hacer el Plan de Seguridad Informática hay que tomar en cuenta el inventario de activos en donde se recogerá los datos de los activos más importantes.

Gráfico: 2.4 Inventario de Activos (Fuente: Poveda, J.M., 2011, pág. 3)

Identificación del activo

Es el código que permitirá ordenar y localizar los activos. (Poveda, J.M., 2011, pág. 3)

Tipo de activo

Constituye la categoría que se mencionó antes, a la que pertenece el activo. (Poveda, J.M., 2011, pág. 3)

Descripción

Una breve descripción del activo para identificarlo. (Poveda, J.M., 2011, pág. 3)

Propietario

Es la persona a cargo del activo, no necesariamente es el dueño del mismo. (Poveda, J.M., 2011, pág. 3)

Localización

Es el lugar donde se encuentra físicamente el activo; para el caso de información en formato electrónico, en qué equipo se encuentra. (Poveda, J.M., 2011, pág. 3)

Valoración de activos

La valoración de activos conocida como valuación de activos según lo define en la norma ISO 27005 en el Anexo B.2; se realiza una vez que se han identificado e implica estimar qué valor tienen para la institución educativa y cuál es su importancia para la misma; y para calcular este valor, se considera cual puede ser la afectación que puede suponer para la organización que un activo resulte dañado en cuanto a su disponibilidad, integridad y confidencialidad.

"Para la valoración se puede utilizar una escala cuantitativa o cualitativa. Si es posible valorar económicamente los activos, se utiliza la escala cuantitativa. En la mayoría de los casos, no es posible o va a suponer un esfuerzo excesivo, por lo que utilizan escalas cualitativas como por ejemplo: bajo, medio, alto o bien un rango numérico, por ejemplo de 0 a 10." (Poveda, J.M., 2011, pág. 6)

Según la norma ISO 27005: 2008 en el anexo B.2 los criterios a tomar en cuenta para evaluar las posibles consecuencias como resultado de una pérdida de confidencialidad, integridad, disponibilidad entre otras son:

- Violación de las normas establecidas.
- Reducción del rendimiento de la actividad.

- Efecto negativo en la reputación.
- Pérdidas económicas.
- Crisis en el negocio

La valoración debe ser lo más objetiva posible y preparado los criterios (confidencialidad, integridad, disponibilidad entre otros) con anterioridad, por lo que en el proceso deben estar involucradas todas las áreas de la organización, aunque no participen en otras partes del proyecto y de esta manera obtener una imagen realista de los activos de la organización.

2.5.4.4.5 Análisis de Riesgos

El análisis de riesgos comprende la identificación de vulnerabilidades y análisis de amenazas.

Identificación de vulnerabilidades

ISO 27005 define la vulnerabilidad como una debilidad de un activo o grupo de activos que puede ser explotado por una o más amenazas.

Las vulnerabilidades se clasifican en:

- Hardware
  - Susceptibilidad a la humedad
  - Susceptibilidad al polvo
  - Susceptibilidad a la suciedad
  - Susceptibilidad al almacenamiento sin protección
- Software
  - Pruebas insuficientes
  - La falta de seguimiento de auditoría
- Red
  - Líneas de comunicación no protegidas

Arquitectura de red insegura

- Personal

  Proceso de reclutamiento insuficiente

  Conciencia de seguridad inadecuada

- Sitio

  Zona sujeta a inundaciones

  Fuente de energía poco fiable

- Organizativo

  Falta de auditorías periódicas

  Falta de planes de continuidad

  Falta de seguridad

Análisis de amenazas

"**Amenaza**: Origen, fuente potencial de afectación que causa un incidente no deseado y puede resultar en un daño a un sistema u organización y/o a sus activos." (Bautista, L., 2013, pág. 5), es decir es un mecanismo con la capacidad de quebrantar la seguridad informática o de la información y este mecanismo o acción existirá siempre y cuando esté presente una vulnerabilidad.

El origen de las amenazas según lo define en la norma ISO 27005:2008 puede ser: natural, humano, intencionado, no intencionado.

Tipos de amenazas

A continuación se presenta una lista de tipos de amenazas enunciadas en la noma ISO 27005: 2008.

Tipo	Amenaza
Daño Físico	Fuego
	Daño de agua
	Contaminación
	Accidente grave
	Destrucción de equipos o medios
	Polvo, corrosión, congelación
Eventos naturales	Fenómenos sísmicos
	Fenómenos volcánicos
	Fenómenos meteorológicos
	Inundaciones
Pérdida de servicios esenciales	Peligro del aire acondicionado o sistema de abastecimiento de agua
	Pérdida de energía eléctrica
	Falla en los equipos de telecomunicaciones
Disturbio debido a la radiación	Radiación electromagnética
	Radiación térmica
	Pulsos electromagnéticos
Compromiso de la información	Intercepción de señales comprometidas de interferencia
	Espionaje remoto
	espionaje
	robo de los medios de comunicación o documentos
	Robo de equipos
	la recuperación de los medios de comunicación reciclados o desechados
	Divulgación

Tabla 2.2: Ejemplos de tipos de amenazas (Traducción ISO 27005 - Tannia Mayorga)
(IEC/ITC 27005, 2008, pág. 39)

Tabla 2.2: Ejemplos de tipos de amenazas (Traducción ISO 27005 - Tannia Mayorga) (IEC/ITC 27005, 2008, pág. 39) (cont.)

Tipo	Amenaza
	Datos de fuentes no confiables
	La manipulación del hardware
	La manipulación del software
	Detección de la posición
Fallas técnicas	Daño en el equipo
	Malfuncionamiento del equipo
	Saturación del sistema de información
	Malfuncionamiento del software
	Incumplimiento del mantenimiento del sistema de información
Acciones no autorizadas	Uso de equipo no autorizado
	Copia de software fraudulento
	Uso de falsificación o software copiado
	Corrupción de los datos
	Procesamiento de datos ilegales
Funciones comprometedoras	Error en el uso
	Abuso de derechos
	Forjado de los derechos
	Denegación de acciones
	Incumplimiento de la disponibilidad del personal

Tabla 2.2: Ejemplos de tipos de amenazas (Traducción ISO 27005 - Tannia Mayorga) (IEC/ITC 27005, 2008, pág. 39)

La amenazas de origen humano son las de especial atención como por ejemplo hacker, cracker, criminales informáticos, terrorismo, espionaje industrial entre otras, cuya motivación puede ser el dinero, desafío, rebelión, destrucción de la información, divulgación ilegal, alteración de datos, venganza, curiosidad, errores intencionales, entre otras. (IEC/ITC 27005, 2008, págs. 39-41)

2.5.4.4.6 Plan de seguridad de la información

Políticas

"Política de Seguridad recoge las directrices y objetivos de una organización con respecto a la seguridad de la información. Forma parte de su política general y por tanto, ha de ser aprobada por la dirección" (Aguilera, pág. 21).

Una política de seguridad informática es: "Una serie de sentencias formales o normas, que deben ser cumplidas por todas las personas de una organización que dispongan de acceso a cualquier información, datos o tecnología que sean propiedad de la organización." (IETF, 1997)

2.5.4.5 Metodologías y estándares de evaluación de riesgos

En la siguiente tabla se presenta una comparación tomando en cuenta el idioma, a qué es aplicable, cuál es el enfoque, equipo de medición, comunicación del equipo reunido, recursos humanos, herramientas de software, documentación, análisis de riesgo, tratamiento de riesgo que permite dar una idea general de cuál estándar o estándares aplicar para evaluar riesgos.

	ISO 27005:2008	ISO 27001:2005	NIST SP 800-30	OCTAVE
Idioma	Inglés	Inglés - español	Inglés	Inglés
Aplicable	Todo tipo de organizaciones	Todo tipo de organizaciones	Es más aconsejable para medición de riesgos relacionados con tecnología	La mayoría de organizaciones Elaborada para procesos específicos de evaluación de riesgo los cuales están basados en el conocimiento de las personas.
Enfoque	Análisis de riesgo Cubre personas, procesos y tecnología y es generalmente orientado hacia prácticas gerenciales de alto nivel	Sistema de Gestión	Sistema de gestión Medir riesgos tecnológicos	Método auto dirigido Elaborada para Procesos organizacionales

Tabla 2.3: Metodologías de evaluación del riesgo y estándares (Fuente: Tewari, A., *2013*) (Fuente: IEC, ISO 27001: 2005) (Fuente:IEC, ISO 27005:2008) (Elaborado por: Investigador) (cont.)

Tabla 2.3: Metodologías de evaluación del riesgo y estándares (cont.)

	ISO 27005:2008	ISO 27001:2005	NIST SP 800-30	OCTAVE
Equipo de medición	Menciona los derechos de las personas (tanto técnicos como personal del negocio) que están involucradas en la medición del riesgo	Involucra todo el talento humano de las instituciones que tenga que ver internamente o externamente, otorgando roles y responsabilidades para que el SGSI se aplique.	Menciona roles en metodología pero no crea un equipo de medición	Detalla la creación de un equipo de análisis que comprende tanto las líneas de negocio y el departamento de TI de la organización.
Comunicación de la información reunida	Usa la misma técnica que la NIST 800-30 además de observación de procesos mencionados en políticas organizacionales	Usa la misma técnica que la NIST 800-30 además de observación de procesos mencionados en políticas organizacionales	Usa técnicas típicas para reunir información tales como cuestionarios, entrevistas y revisión de documentación	Usa un enfoque basado en taller para reunir información y tomar decisiones

Tabla 2.3: Metodologías de evaluación del riesgo y estándares (Fuente: Tewari, A., *2013*) (Fuente: IEC, ISO 27001: 2005) (Fuente:IEC, ISO 27005:2008) (Elaborado por: Investigador) (cont.)

Tabla 2.3: Metodologías de evaluación del riesgo y estándares (cont.)

	ISO 27005:2008	ISO 27001:2005	NIST SP 800-30	OCTAVE
Recursos Humanos	Específicamente cubre seguridad de recursos humanos lo cual incluye empleados, contratistas y terceros- usuarios que tengan que ver con el negocio	Presenta una lista de Controles para recursos humanos cuyo objetivo es asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades, y sean adecuados para los roles para los cuales se les considera; y el riesgo de robo, fraude o mal uso de los medios	No se ocupa de los recursos humanos como posible activo de la organización	Método que busca identificar recursos humanos que puede ser un activo "misión-crítica" con respecto a problemas de TI.

Tabla 2.3: Metodologías de evaluación del riesgo y estándares (Fuente: Tewari, A., *2013*) (Fuente: IEC, ISO 27001: 2005) (Fuente:IEC, ISO 27005:2008) (Elaborado por: Investigador) (cont.)

Tabla 2.3: Metodologías de evaluación del riesgo y estándares (cont.)

	ISO 27005:2008	ISO 27001:2005	NIST SP 800-30	OCTAVE
Herramientas de software	Sistema de uso y herramientas de auditoría de redes para comprobación de cumplimiento		Se basa en la definición de roles para determinar el uso para propósitos de prueba	Usa un taller de 5 procesos, cuyos participantes son principalmente el equipo núcleo, para usar herramientas de software especialmente para identificar previamente vulnerabilidades
Documentación	Cubre todos los controles de seguridad definidos en el estándar ISO 27002	Cubre todos los descritos en la ISO 27005, ISO 27002	Desarrolla listas de chequeo de reque-rimientos de seguridad para las áreas de seguridad de gerencia operacional y técnica	Se basa en la creación de 3 catálogos

Tabla 2.3: Metodologías de evaluación del riesgo y estándares (Fuente: Tewari, A., *2013*) (Fuente: IEC, ISO 27001: 2005) (Fuente:IEC, ISO 27005:2008) (Elaborado por: Investigador) (cont.)

Tabla 2.3: Metodologías de evaluación del riesgo y estándares (cont.)

	ISO 27005:2008	ISO 27001:2005	NIST SP 800-30	OCTAVE
Análisis de riesgo	Análisis de riesgo • Identificación del riesgo • Estimación del riesgo Evaluación de riesgo	Utiliza el apoyo de la ISO 27005 para dicho proceso que es parte del plan de seguridad de información que es el primer paso Establecer el SGSI	1. Caracterización del sistema 2. Identificación de la amenaza 3. Identificación de vulnerabilidades 4. Análisis de controles 5. Determinación de la probabilidad 6. Análisis de impacto 7. Determinación del riesgo 8. Control de recomendaciones	**Fase 1**: Construir perfiles de amenazas basadas en activos (evaluación organizacional). 1. Identificar los conocimientos de la gestión Senior 2. Identificar el conocimiento del área de gestión operacional 3. Identificar los conocimiento del personal 4. Crear un perfil de amenazas **Fase 2**:Identificar vulnerabilidades de infraestructura (evaluación tecnológica 5. Identificar componentes claves Evaluar componentes seleccionados

Tabla 2.3: Metodologías de evaluación del riesgo y estándares (Fuente: Tewari, A., *2013*) (Fuente: IEC, ISO 27001: 2005) (Fuente:IEC, ISO 27005:2008) (Elaborado por: Investigador) (cont.)

Tabla 2.3: Metodologías de evaluación del riesgo y estándares (cont.)

	ISO 27005:2008	**ISO 27001:2005**	**NIST SP 800-30**	**OCTAVE**
… **Análisis de riesgo**			9. Documentación de Resultados	
Tratamiento del riesgo	Reducir Retener Evitar Transferir	Trabaja en base a la norma ISO 27005	• Asumir el riesgo • Evitar el riesgo • Limitar el riesgo • Planear el riesgo • Reevaluar y confirmar • Transferir el riesgo	**Fase 3:** Desarrollar estrategias de seguridad y planes de mitigación (estrategia y plan de desarrollo). 6. Conducir el análisis de riesgo Desarrollo del plan de protección

Tabla 2.3: Metodologías de evaluación del riesgo y estándares (Fuente: Tewari, A., *2013*) (Fuente: IEC, ISO 27001: 2005) (Fuente:IEC, ISO 27005:2008) (Elaborado por: Investigador)

2.5.5 Categorías de la variable Dependiente

2.5.5.1 **Internet**

Internet viene de la palabra compuesta por el prefijo "inter-" y "*networking*" (conexión en red) es una 'red de redes' que conecta a millones de ordenadores alrededor del mundo, está disponible para cualquier persona, como por ejemplo compañías de negocios, universidades, instituciones del gobierno, entidades comerciales entre otros; convirtiéndose en una red mundial compartida por todos sus usuarios para intercambiar mensajes electrónicos, correos, información, música, videos, imágenes. (Universidad de Jaén, 2013, págs. 73, sección 5.5 primer al cuarto párrafo).

En el año 2006 sale una publicación en la revista de Universidad y Sociedad del Conocimiento de autoría de Joseph M. Duart donde hace mención a que "el uso educativo de Internet pasa por la incorporación de la tecnología, como herramienta o como soporte, en la metodología docente y de aprendizaje" (Duart, J., 2006, pág. 5to párrafo) , yo diría que ahora que estamos en el año 2013 en Ecuador sigue siendo pasado por alto el uso de las herramientas de poyo en el aula que promuevan la reflexión en los estudiantes lo que convierte al uso del internet en un vulnerabilidad en el aula si no es aplicado usando las herramientas como webquests, cazas de tesoro.

El Internet empezó con fines militares, para después convertirse en una gran herramienta útil para la investigación, para la formación de personas, para hacer negocios, compras, ventas, entre otros; contiene tanta información y formas de comunicarse, a continuación se analiza las ventajas e inconvenientes de la introducción de Internet a los procesos formativos.

2.5.5.1.1 Ventajas, inconvenientes, riesgos

A continuación una tabla en la que Barroso (2004, p. 153), presenta ventajas e inconvenientes de la introducción de Internet a los procesos formativos.

Ventajas	Inconvenientes
La formación se centra en el estudiante y se adapta a sus características y necesidades. Conecta a estudiantes dispersos geográficamente. El contenido puede ser actualizado y adaptado de forma rápida y económica.	Costo de los equipos. Se requiere contar con un personal técnico de apoyo. Necesidad de cierta formación para poder interaccionar en un entorno telemático. Necesidad de adaptarse a nuevos métodos de aprendizaje.
Reducción de costos económicos. Ofrece flexibilidad para la formación. El ritmo de aprendizaje es marcado por el estudiante sin que ello no signifique que no pueda existir una propuesta por parte de los instructores. Se amplían los escenarios para el aprendizaje: centro educativo, trabajo y hogar. Permite la combinación de diferentes recursos multimedia. Y la posibilidad de utilizar diferentes herramientas de comunicación sincrónica y asincrónica para comunicarse el estudiante con otros estudiantes y con el profesor.	Problemas de derechos de autor, seguridad y autoría científica. El ancho de banda generalmente no permite realizar una verdadera comunicación audiovisual y multimedia; toma más tiempo y dinero el desarrollo que la distribución. Muchos de los entornos son demasiado estáticos y simplemente consisten en ficheros en formato texto o pdf. Si los materiales no se diseñan de forma específica se puede caer en la potenciación del aprendizaje memorístico. Y la falta de experiencia educativa en su consideración como medio formativo.

Tabla 2.4 Ventajas e inconvenientes de la introducción de la red Internet en los procesos formativos (Fuente: Barroso, 2004, pág. 153)

Riesgos de niños, niñas y adolescentes al navegar en Internet

Según el gobierno argentino, en una investigación realizada en el año 2009, el Programa nacional de infraestructuras críticas de información y ciberseguridad, presenta el documento titulado "Navegación Segura y uso responsable de Internet", donde exponen los siguientes riesgos de niños, niñas y adolescentes al navegar en Internet:

Riesgo	Descripción
Violación a la intimidad	La exposición de mucha información personal sin restricciones representa un riesgo si esos datos son utilizados con fines maliciosos o para provocar daños o realizar estafas y secuestros, entre otras conductas delictivas.
Robo o suplantación de identidad	Tras la obtención de datos personales de niños, niñas y adolescentes, así como de otros integrantes de la familia, los menores pueden ser utilizados para sustraer una identidad de otros y, en consecuencia, efectuar acciones en nombre de otra persona. Dichas acciones pueden estar orientadas a ocasionar daños económicos (por ejemplo: la compra por Internet con los datos de pago de un tercero) o morales (por ejemplo: la participación en un foro identificándose como otra persona)
Abuso emocional	Con el objeto de establecer una relación de confianza, personas inescrupulosas acercan a los menores materiales audiovisuales con contenido violento, pornográfico o sexual, en forma distorsionada o simulada, usando dibujos animados u otro tipo de formato destinado a la comunicación infantil o adolescente.

Tabla 2.5: Riesgos de niños, niñas y adolescentes al navegar en Internet (Fuente: Gobierno de Argentina, 2009, págs. 5-7) (cont.)

Tabla 2.5: Riesgos de niños, niñas y adolescentes al navegar en Internet (cont.)

Riesgo	Descripción
Abuso emocional	… De este modo buscan reducir cualquier posible resistencia, atraer o generar una relación de confianza para luego cometer otros delitos. También podrían obtener cierta información con el fin de utilizarla después para extorsionar al menor y obligarlo a realizar determinadas acciones, comprometiendo así su integridad
Abuso sexual i/o violencia	Mediante el anonimato que brinda Internet, abusadores y pedófilos entablan relaciones virtuales con niños, niñas y adolescentes, para luego coordinar encuentros reales en los que podrían abusar sexualmente del menor o llevar a cabo otras acciones violentas
Exposición a material inadecuado o engañoso	Internet es una gran fuente de contenidos, de carácter irrestricto. Todo niño, niña o adolescente que navegue libremente puede quedar expuesto a material inapropiado para su edad y nivel de maduración, contrario a la idiosincrasia familiar u opuesto a la orientación con que su familia ha establecido abordar temas como drogadicción, racismo, sexualidad o religión. Ejemplos de estos contenidos se encuentran en sitios con lenguaje hostil e inapropiado, imágenes violentas, textos en los que se hace apología de las drogas, intención discriminatoria, pornografía, hábitos dañinos de alimentación, entre otros.

Tabla 2.5: Riesgos de niños, niñas y adolescentes al navegar en Internet (Fuente: Gobierno de Argentina, 2009, págs. 5-7) (cont.)

Tabla 2.5: Riesgos de niños, niñas y adolescentes al navegar en Internet (cont.)

Riesgo	Descripción
Acoso entre pares usando las nuevas Tecnologías de la Información y Comunicación (TIC) o "cyberbulling"	Acoso entre pares usando las nuevas Tecnologías de la Información y Comunicación (TIC) o "cyberbulling". La facilidad de acceso a la tecnología permite que pueda ser utilizada por los mismos niños para incomodar o atemorizar a otros menores (por ejemplo, mediante mensajes de texto –SMS- o correos electrónicos incesantes). Esto puede ocasionar daños o trastornos psicológicos en las víctimas, que merecen atención por parte de adultos, docentes y toda la comunidad.
Infracción a leyes, normas o disposiciones	Copiar material protegido bajo derechos de autor sin la debida autorización o descargar archivos de las más variadas características (películas, software o música) es una práctica que, por desconocimiento o descuido, puede comprometer a los menores y sus familias, llevándolos a situaciones con implicancias judiciales e inclusive a cometer delitos. Además, la mayor parte de la información que encontramos en Internet y su presentación no tienen garantías de certeza, razón por la cual es importante realizar verificaciones sobre la fuente y buscar otras referencias sobre las consultas realizadas en la web.

Tabla 2.5 : Riesgos de niños, niñas y adolescentes al navegar en Internet (Fuente: Gobierno de Argentina, 2009, págs. 5-7)

2.5.5.2 **Herramientas de apoyo**

Las herramientas de apoyo son instrumentos, procedimientos que el docente utiliza para dar sus clases y que incrementa las habilidades en el maestro en el momento de dictar las mismas o realizar determinadas tareas como por ejemplo prezzi, slideshare, Microsoft Office, software educativo, enciclopedias, videos, canciones, textos, material didáctico entre otras (Definición ABC, 2007).

2.5.5.3 **Formación de niños, niñas y adolescentes**

El término Formación puede ser enfocado desde varios aspectos como son militar, psicológico, económico, social, geológico entre otros; para el desarrollo de esta investigación se tomará como sinónimo de educación, de esta forma puedo decir que tiene un origen latino o proviene de la palabra formatio, se asocia al verbo formar (Wordp, 2008, pág. 1), o también puede ser considerado como una secuencia de pasos que consiste en proporcionar conocimientos.

La formación de niños, niñas y adolescentes constituye una secuencia de pasos, técnicas, procedimientos para proporcionar conocimientos a los niños, niñas y adolescentes durante la etapa de educación básica que le permitan prepararles para su siguiente formación que constituye el bachillerato, o a su vez preparar en el proceso de la búsqueda del "aprender a aprender". (Larousse, 2009).

2.5.5.3.1 Educación

Educar viene de la palabra educare cuyo significado es sacar afuera y se puede decir que la educación es el camino que siguen los seres humanos para formarse y definirse como personas; reviste particularidades esenciales según los rasgos de el niño, niña o adolescente; hoy en día conlleva también ciertos riesgos sociales debido a la amplia libertad y soledad por la que atraviesa el ser humano, especialmente los adolescentes; la educación necesita

ser más firme y exigente ya que los estudiantes requieren poner mucho empeño para aprender y desarrollar todo su potencial para enfrentarse a las competencias tecnológicas que la era contemporánea requieren (Jaramillo, P, 2009).

Tipos

Para efectos de esta investigación se consideran únicamente los siguientes tipos de educación: inicial y básica.

Educación Inicial

"La Educación Inicial es el proceso de acompañamiento al desarrollo integral de niños y niñas menores de 5 años, y tiene como objetivo potenciar su aprendizaje y promover su bienestar mediante experiencias significativas y oportunas que se dan en ambientes estimulantes, saludables y seguros." (Ministerio de Educación del Ecuador, 2013)

Educación General Básica

"La Educación General Básica en el Ecuador abarca diez niveles de estudio, desde primer grado hasta décimo. Las personas que terminan este nivel, serán capaces de continuar los estudios de Bachillerato y participar en la vida política y social, conscientes de su rol histórico como ciudadanos ecuatorianos." (Ministerio de Educación de Ecuador)

Recursos Tecnológicos

Definición

Los recursos tecnológicos constituyen la tecnología que puede ser usada por el docente y sirve de beneficio para el desenvolvimiento de sus funciones; ayudan a que los contenidos sean difundidos a los estudiantes de una manera interactiva y divertida, como por ejemplo

Proyector, Laptop, computador, Smart boards, DVD, Ipad entre otros; de esta forma los estudiantes aceleran el proceso de aprendizaje.

2.5.5.4 Internet como herramienta de apoyo en la formación de niños, niñas y adolescentes

2.5.5.4.1 Definición

Es una red de redes con abundante información escrita, visual, contenido multimedia (videos, sonidos, animaciones) que con cierta estructura puede ser usada como material de apoyo en el aula de clase o fuera de ella, para educar a niños, niñas y adolescentes a "aprender a aprender" gracias a los servicios que ofrece la www que ha ido evolucionando como se puede ver a continuación.

2.5.5.4.2 www

La world wide web conocida como www, fue lo que hizo posible que Internet abarcara a todo el planeta, fue desarrollada en 1990 por el programador inglés, Tim Berners-Lee, como se puede ver en la tabla 2.6 , donde Carlos Guazmayán Ruiz en su libro "Internet y la Investigación científica" (pg. 26-28).

Posterior a ello en la educación empieza a utilizarse la web 1.0, web 2.0 y actualmente la web 3.0.

2.5.5.4.3 Web 1.0

La web 1.0 se conocía como la tecnología de acceso ya que permitía únicamente lectura de información en el Internet, es decir solamente los webmasters podían modificar la misma, esta estaba disponible para la educación como una gran biblioteca con información útil para investigación a nivel mundial; se podía utilizar los navegadores para búsqueda (Rosique, R, pág. 3).

Historia de la www

Año	Descripción
1968	Ted Nelson, ideó un hipertexto de información interrelacionada , creó un sistema utópico "Xanadú": un hipertexto abierto y autoevolutivo que tenía por objeto enlazar toda la información pasada, presente y futura del planeta.
1969	Se había establecido una red de comunicación entre ordenadores
Finales de los 70	Se habían formado varias comunidades interactivas de científicos y hackers, para la gente, para las empresas y para la sociedad en general
Años 80	Bill Atkinson, autor de la interfaz gráfica de Macintosh, desarrolló el sistema HyperCard para interrelacionar información
1980	Berners-Lee perfeccionó el programa Enquire; definió y elaboró el software que permitía sacar e introducir información de y en cualquier ordenador conectado a través de Internet (HTTP, HTML, URI, denominado depués URL)
1990	Berners-Lee en colaboración con Robert Cailliau, desarrollaron su navegador editor cuyo nombre fue world wide web al sistema de hipertexto.
1991	CERN divulga en la red el software WWW en agosto de 1991.
1992	Aparece Erwise la primera versión modificada, desarrollada en el Instituto Tecnológico de Helsinki en abril de 1992.
1993	Marc Andressen y, Eric Bina diseñaron Mosaic e incluyeron una capacidad gráfica avanzada para poder obtener y distribuir imágenes a través de Internet, e hicieron público su software Usenet en enero de 1993, en forma gratuita como la world wide web.

Tabla 2.6 Historia de la www (Fuente: : Guazmayán, C., 2004, págs. 26-28) (cont.)

Tabla 2.6 Historia de la www (cont.)

1994	Gracias a la creación de la empresa Mosaic Comunications cuyos miembros fueron Andressen, Bina y otros miembros del equipo aparece Netscape Comunications, que fue la compañía que puso en red el primer navegador comercial, Nescape Navigator en octubre de 1994.
1995	Divulgaron el software Navigator a través de la red, gratis para usos educativos y a un coste de 39 dólares para las empresas.
	Microsoft incluyó junto a su software Windows 95 su propio navegador, Internet Explorer
	Internet nació en 1995

Tabla 2.6: Historia de la www (Fuente: Guazmayán, C., 2004, págs. 26-28)

2.5.5.4.4 Web 2.0

Conocida como la tecnología de participación, permite a los usuarios interactuar con otros usuarios, es decir permite utilizar la inteligencia colectiva para proporcionar servicios interactivos en la Red, pueden cambiar el contenido del sitio web a los que tienen permiso para emitir comentarios, opiniones o son de autoría propia. (Rosique, R, págs. 3-4).

2.5.5.4.5 Web 3.0

Se evidencia una evolución en la interacción sobre la red lo que incluye la transformación de la red en una base de datos, un movimiento hacia hacer los contenidos accesibles por múltiples aplicaciones que no son buscadores, el empuje de las tecnologías de inteligencia artificial, la web semántica, la web geoespacial.

"Se busca que la plataforma Web se convierte al mismo tiempo en una plataforma de desarrollo: más inteligente, más personalizada, más contextualizada y por ende más interrelacionada con la educación" . (Rosique, R, pág. 5).

2.5.5.5 **TICs**

2.5.5.5.1 Definición

Tics son las iniciales de Tecnologías de la Información y Comunicaciones.

2.5.5.5.2 Uso de la web en la clase

El uso de la web en la clase "Román y Llorente (2007) argumentan que las denominadas webquest, cazas de tesoros, blogs y wikis son e-actividades pues son aspectos metodológicos basados en el constructivismo, es decir que la finalidad de todas éstas es que el alumno se convierta en el protagonista de su aprendizaje."; usar la web en el aula es la competencia digital que un docente debe tener para dar clases a niños, niñas y adolescentes que son nativos digitales, y aprender a usar la web para "aprender a aprender" es la destreza que los niños, niñas y adolescentes deben aprender, a través del uso de las e-actividades que menciona Román y Llorente.

Webquest

"Una WebQuest es un tipo de actividad didáctica basada en presupuestos constructivistas del aprendizaje y la enseñanza que se basa en técnicas de trabajo en grupo por proyectos y en la investigación como actividades básicas de enseñanza/aprendizaje. Su mecánica es relativamente simple y nos remite a prácticas bien conocidas y asentadas de trabajo en el aula" (Segura, J, 2005) . Las partes de una webquest son: introducción, tareas, proceso, recursos, evaluación, conclusión.

Caza de tesoro

"La "caza del tesoro" consiste en una hoja de trabajo con una serie de preguntas y una lista de enlaces en sitios de Internet donde los alumnos habrán de buscar las respuestas. La actividad se cierra con la "gran pregunta", cuya respuesta no se puede obtener directamente a partir de la información extraída a lo largo de la actividad, sino que se ha de construir

relacionando la información obtenida con conocimientos previos y con el propio punto de vista." (Zayas, F., Esteve, P.P., 2010, pág. 1). La estructura para la realización de la "caza" tiene la siguiente estructura: Introducción, Preguntas, Recursos, La "Gran Pregunta" y Evaluación.

Wikis

Wiki, proviene del hawaiano: wiki-wiki, rápido, expresión repetida por los remeros de las canoas, es considerado un sistema de gestión de contenidos en la red (Ruíz Palmero, 2008, p.49), por ejemplo la Wikipedia.

Blog

Es un sitio web frecuentemente actualizado donde se recopila textos o artículos de varios autores, donde el más reciente aparece primero, y constituyen una herramienta potencial didáctica para la enseñanza. (Valero, A., 2008)

2.5.5.6 **Telecomunicaciones**

2.5.5.6.1 Definición

"Abarca todas las formas de comunicación a distancia. La palabra incluye el prefijo griego tele, que significa "distancia" o "lejos". Por lo tanto, la telecomunicación es una técnica que consiste en la transmisión de un mensaje desde un punto hacia otro, usualmente con la característica adicional de ser bidireccional. La telefonía, la radio, la televisión y la transmisión de datos a través de computadoras son parte del sector de las telecomunicaciones." (Ecured, 2011)

2.5.5.6.2 Transmisión de datos e interconexión entre computadores

Considerando la transmisión de datos e interconexión entre computadores como parte de las Telecomunicaciones se puede decir que esta comunicación mediante computadores (CMC)

en inglés Computer Mediated Comunication puede realizarse en forma síncrona o asíncrona.

Comunicación síncrona

La comunicación síncrona es la que realiza en tiempo real, en lo que compete a esta investigación al Internet, el exponente principal es el chat.

Comunicación asíncrona

La comunicación asíncrona es la que no se realiza en tiempo real, relacionando al Internet se encuentra como ejemplo principal el correo electrónico.

Ejemplos de comunicación síncrona y asíncrona:

Comunicación síncrona	Comunicación asíncrona
Chat	Correo electrónico
MOOs	Correo de voz
Audio conferencia	Grupo de noticias
Video conferencia	Foros de debate

Tabla 2.7: Ejemplos de servicios del Internet categorizados por la forma de comunicación: síncrona, asíncrona (Fuente: Universidad de Jaén, 2013, págs. 53-61) (Elaborado por: Investigador)

2.6 Hipótesis

Hi: La seguridad informática incide en la utilización de Internet como herramienta de apoyo en la formación de niños, niñas y adolescentes de Educación Inicial y Básica del Centro Educativo La Pradera.

H0: La seguridad informática no incide en la utilización de Internet como herramienta de apoyo en la formación de niños, niñas y adolescentes de Educación Inicial y Básica del Centro Educativo La Pradera.

2.7 Señalamiento de variables de la hipótesis

Variable independiente: Seguridad informática.

Variable dependiente: Internet como herramienta de apoyo en la formación de niños, niñas y adolescentes.

CAPÍTULO III

METODOLOGÍA

3.1 Enfoque

Esta investigación tiene un enfoque cuali-cuantitativo porque la investigación se enfoca en la medición de la seguridad informática en el CELP.

3.2 Modalidad de Investigación

Se aplicará investigación de campo porque se va a aplicar en el lugar donde se suscita el problema; investigación bibliográfica ya que se va a investigar en la comunidad científica qué tipo de formación permite la informática en los niños, niñas y adolescentes y de esta forma apoyará el desarrollo del objetivo principal de esta investigación.

Se pretende hacer un diagnóstico de la situación actual usando técnicas como observación, entrevistas, encuestas para recopilar información y de esa forma hacer la propuesta de las políticas, normas procedimientos, estándares de seguridad informática para la utilización de Internet como herramienta de apoyo que permita mejorar la formación de niños, niñas y adolescentes de educación inicial y básica; e indagar qué tipo de formación permite la informática en los niños, niñas y adolescentes.

3.3 Nivel o tipo de investigación

Se aplicará investigación:

- **Exploratoria** ya que es un tema de interés para el área educativa (Lozano, 2008, págs. 1-2).
- **Descriptiva** o estadística ya que en base a los datos obtenidos se pretende determinar cómo incide la seguridad informática y el internet como herramienta de apoyo en la formación de niños, niñas y adolescentes y probar las hipótesis planteadas y es basada en la observación.
- **Explicativa** ya que tiene relación causal y se analizarán las amenazas y vulnerabilidades existentes en la Institución para después hacer la propuesta de políticas a ser aplicadas para garantizar la seguridad informática.
- **Correlacional** ya que se pretende establecer la relación entre la seguridad informática y el internet como herramienta de apoyo en la formación de niños, niñas y adolescentes.

3.4 Población y muestra

Descripción	Muestra	Población
Propietario – Director	1	1
Personal Docente de inicial	1	1
Personal Docente de educación básica	7	10
Personal Administrativo	3	3
Responsable Tecnología	1	1
Profesor de Tics	1	1
Estudiantes	26	150
TOTAL	40	167

Tabla 3.1 Población y muestra (Elaborado por: Investigador)

3.5 Operacionalización de variables

3.5.1 Variable Independiente:

Seguridad Informática

Conceptualización	Dimensiones	Indicadores	Items básicos	Técnicas e instrumentos
Consiste en asegurar que los recursos tecnológicos (hardware, información y programas, red) de una organización sean utilizados de forma adecuada y que el acceso a la información almacenada; así como la modificación de la misma, solo pueda ser realizado por personal autorizado.	Hardware	Disponibilidad Confidencialidad Integridad	¿El hardware a su cargo o que utiliza está disponible cuando lo necesita? ¿Qué pasaría si en el servidor de aplicaciones fueran modificadas las cuentas de usuario? ¿Cuál es la importancia que se diera si alguien accede al activo (computador, impresora, información, laboratorio de Tics, entre otros) que usted usa o está a su cargo de manera no autorizada?	Encuesta dirigida al personal docente y administrativo (cuestionario)

Tabla 3.2: Variable Independiente (Elaborado por: Investigador) (cont.)

Tabla 3.2: Variable Independiente (cont.)

Conceptualización	Dimensiones	Indicadores	Items básicos	Técnicas e instrumentos
	Hardware	Espacio físico	El lugar donde se encuentran los equipos es adecuado y seguro.	Observación (Guía de la observación)
		Tecnología	¿Qué tecnología dispone el CELP?	
	Software	Educativo	Software educativo del CELP Cuentan con programas o sistemas que ayuden a los docentes en la formación académica de los estudiantes	Observación (Guía de la observa
		Licencias	¿El software con el que cuenta la institución tiene licencias de uso? ¿Dispone de un sistema operativo multiusuario instalado en el servidor de aplicaciones?	Entrevista al encargado de tecnología

Tabla 3.2: Variable Independiente (Elaborado por: Investigador) (cont.)

Tabla 3.2: Variable Independiente (cont.)

Conceptualización	Dimensiones	Indicadores	Items básicos	Técnicas e instrumentos
	Software	Tipo	¿El Software es de tipo Freeware, Shareware, Propietario, Libre o Free, Open source, Oculto?	…
		Calidad	¿El Sistema instalado en la institución es de fácil manejo? ¿El tiempo de respuesta es adecuado en el procesamiento de la información? Existe calidad de software en el CELP.	Entrevista al Encargado de Tecnología, Desarrollador Observación
		Seguridad	Antivirus instalado en todos los equipos del CELP Actualización periódica de antivirus en los equipos del CELP. Software que mejore la seguridad informática del CELP	Observación

Tabla 3.2: Variable Independiente (Elaborado por: Investigador) (cont.)

Tabla 3.2: Variable Independiente (cont.)

Conceptualización	Dimensiones	Indicadores	Items básicos	Técnicas e instrumentos
	Software	… Seguridad	¿La versión instalada del software de la base de datos está soportado por el proveedor? ¿Es monitoreada la base de datos constantemente? ¿Tiene instalado software que garantice seguridad para la Gestión de Base de Datos (perfiles de usuario, vistas)? ¿La Base de Datos maneja un alto grado de seguridad de tal forma que garantice la integridad y confidencialidad?	Entrevista al encargado de tecnología
		Sistema de gestión de información	¿Existen políticas para la creación de usuarios y perfiles de acceso en el sistema? ¿Qué tipo de encriptación de claves maneja el sistema? ¿Qué nivel de seguridad maneja el sistema?	Entrevista al encargado de tecnología y al desarrollador del sistema
	Información	Base de datos	¿Existe seguridad para el acceso a la base de datos?	

Tabla 3.2: Variable Independiente (Elaborado por: Investigador) (cont.)

Tabla 3.2: Seguridad informática (cont.)

Conceptualización	Dimensiones	Indicadores	Items básicos	Técnicas e instrumentos
	Información	Respaldos	¿Quién es el encargado(a) de respaldar la información? ¿Realizan copias de seguridad de la información en forma periódica? ¿Existen definidos procedimientos para realizar copias de seguridad de la información? ¿Existe un lugar seguro fuera de la institución donde permanezca una copia de los respaldos de la información? ¿Cuenta la institución con un plan de contingencia ante recuperación de desastres?	Entrevista al encargado de tecnología
	Red	Acceso	¿Los docentes tienen acceso a la red? ¿Existen políticas que permitan hacer un uso adecuado de la Red?	Entrevista al profesor de Tics

Tabla 3.2: Variable Independiente (Elaborado por: Investigador) (cont.)

Tabla 3.2: Seguridad informática (cont.)

Conceptualización	Dimensiones	Indicadores	Items básicos	Técnicas e instrumentos
	Red	Acceso	¿Existen bitácoras para el control del uso de internet en el laboratorio de computación? ¿Existe algún procedimiento para que un docente, utilice Internet en el laboratorio? ¿Tienen definido un procedimiento cuando se presentan problemas de red o internet? ¿Existe algún mecanismo que permita compartir internet de manera segura y además que se evite el acceso a sitios web que se encuentren en listas negras?	Entrevista al profesor de Tics

Tabla 3.2: Variable Independiente (Elaborado por: Investigador) (cont.)

Tabla 3.2: Seguridad informática (cont.)

Conceptualización	Dimensiones	Indicadores	Items básicos	Técnicas e instrumentos
	Red	Acceso	¿Existe una persona encargada de la administración del control de acceso a Internet? ¿Realizan la revisión periódica de los logs de acceso a Internet? ¿En los logs pueden identificar qué equipo accedió a ciertas páginas? ¿Existe restricción en el proxy a páginas inseguras?	Entrevista al Profesor de TIcs

Tabla 3.2: Variable Independiente (Elaborado por: Investigador)

3.5.2 Variable Dependiente:

Internet como herramienta de apoyo en la formación de niños, niñas y adolescentes.

Conceptualización	Dimensión	Indicadores	Ítems	Técnicas e Instrumentos
Es una red de redes que constituye un recurso tecnológico del que se puede conseguir abundante información escrita, visual, contenido multimedia que con cierta estructura puede ser usada como material de apoyo en el aula de clase o fuera de ella, para educar a niños, niñas y adolescentes a "aprender a aprender".	Recursos Tecnológicos	Internet	¿Cree usted que los recursos tecnológicos con que cuenta el Centro Educativo para navegar en Internet son adecuados para utilizarlos como herramienta en la formación de los alumnos? ¿Los estudiantes cuando da sus clases usando Internet, se encuentran expuestos a peligros?	Encuestas al personal docente

Tabla 3.3: Variable dependiente (Elaborado por: Investigador) (cont.)

Tabla 3.3: Variable dependiente (Elaborado por: Investigador) (cont.)

Conceptualización	Dimensión	Indicadores	Ítems	Técnicas e Instrumentos
	Recursos tecnológico	TIC	¿Considera que las Tics son una ayuda para la Educación de los alumnos del CELP	Encuesta al personal docente
		Equipos de tecnología	¿Tiene acceso al uso de computadores en el CELP para dar sus clases o para uso investigativo?	
	Herramienta de apoyo	Herramientas de búsqueda guiada	¿Ha usado Herramientas de búsqueda guiada para las investigaciones y clases de sus estudiantes como Webquest o Casa de Tesoro?	Encuesta al personal docente

Tabla 3.3: Variable dependiente (Elaborado por: Investigador)

3.6 Plan de recolección de información

PREGUNTAS BÁSICAS	EXPLICACIÓN
¿Para qué?	Para alcanzar los objetivos de la investigación
¿De qué personas u objetos?	Dueño de la Institución Directora Inspectora Personal Docente Encargado del Laboratorio Estudiantes
¿Sobre qué aspectos?	Indicadores
¿Quién, quienes?	El investigador
¿Cuándo?	Octubre 2013
¿Dónde?	Centro Educativo La Pradera
¿Cuántas veces?	Una
¿Qué técnicas de recolección?	Entrevista Encuestas Observación
¿Con qué?	Guía de entrevista Cuestionario Inspecciones
¿En qué situación?	Condiciones Circunstancias

Tabla 3.4: Recolección de la información (Elaborado por: Investigador)

3.7 Plan de procesamiento de la información

Para el procesamiento de la información se utilizará herramientas informáticas, para el diseño de tablas y gráficos, la herramienta Excel para realizar gráficas estadísticas lo que cada uno de los encuestados desea expresar.

Proceso:

- Revisión de la información recogida.
- Tabulación de la información obtenida.
- Elaboración de cuadros y gráficos.

Análisis

- Análisis de resultados estadísticos, destacando tendencias o relaciones fundamentales de acuerdo a los objetivos del tema.
- Interpretación de resultados obtenidos.
- Comprobación de hipótesis.
- Conclusiones y recomendaciones.

CAPÍTULO IV

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

4.1 Análisis de resultados

4.1.1 Encuesta dirigida al Personal docente y administrativo sobre valoración de activos

4.1.1.1 Dimensión: Hardware

4.1.1.1.1 Indicador: Disponibilidad

Pregunta: ¿Cuál sería la importancia o el trastorno que tendría que el computador que tiene a su cargo o que maneja no estuviera disponible para dictar su clase?

No aplica o no es relevante	Debe estar disponible al menos el 10% de tiempo	Debe estar disponible al menos el 50% de tiempo	Debe estar disponible al menos el 99% de tiempo
0	1	2	7

Tabla 4.1: Tabulación de encuesta dirigida al Personal Docente y Administrativo referente Disponibilidad de equipos (Elaborado por: Investigador)

A continuación se presenta la gráfica de la tabla 4.1

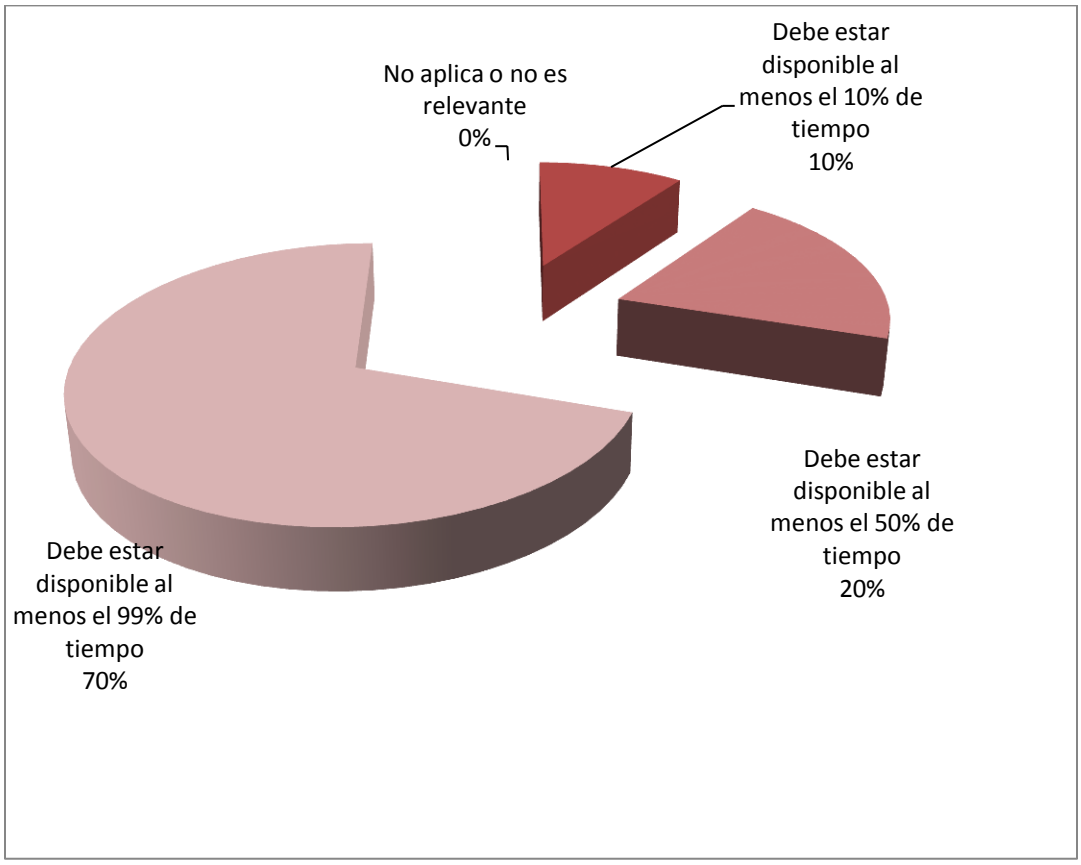


Gráfico: 4.1 Disponibilidad de equipos (Elaborado por: Investigador)

De una muestra de 10 docentes se concluye lo siguiente:

El 70% considera que debe estar disponible el computador para dar clases al menos el 99% del tiempo, mientras que el 20% considera que debe estar disponible al menos el 50% del tiempo, el 10% considera que debe estar disponible al menos el 0% de tiempo; el 0% considera que no aplica o no es relevante.

Pregunta: ¿Cuál sería la importancia o el trastorno que tendría que el servicio de Internet no esté disponible?

No aplica o no es relevante	Debe estar disponible al menos el 10% de tiempo	Debe estar disponible al menos el 50% de tiempo	Debe estar disponible al menos el 99% de tiempo
0	1	1	8

Tabla 4.2: Tabulación de encuesta dirigida al Personal Docente y Administrativo referente Disponibilidad de Internet (Elaborado por: Investigador)

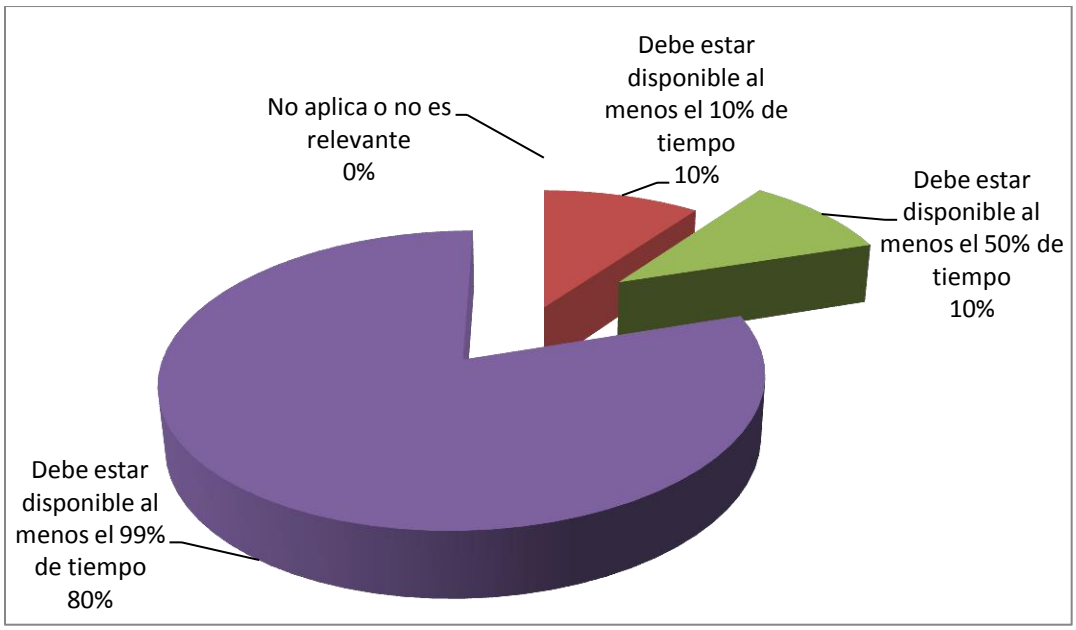


Gráfico: 4.2: Disponibilidad de Servicio de Internet (Elaborado por: Investigador)

El 10% considera que debe estar disponible el servicio de internet para dar clases al menos el 10% del tiempo, mientras que el 80% considera que debe estar disponible al menos el 99% del tiempo y el 10% considera que debe estar disponible al menos el 10%.

Pregunta: ¿Cuál sería la importancia o el trastorno que tendría que el servicio telefónico no esté disponible?

No aplica o no es relevante	Debe estar disponible al menos el 10% de tiempo	Debe estar disponible al menos el 50% de tiempo	Debe estar disponible al menos el 99% de tiempo
0	1	0	9

Tabla 4.3 : Tabulación de encuesta dirigida al Personal Docente y Administrativo referente Disponibilidad de servicio telefónico (Elaborado por Investigador)

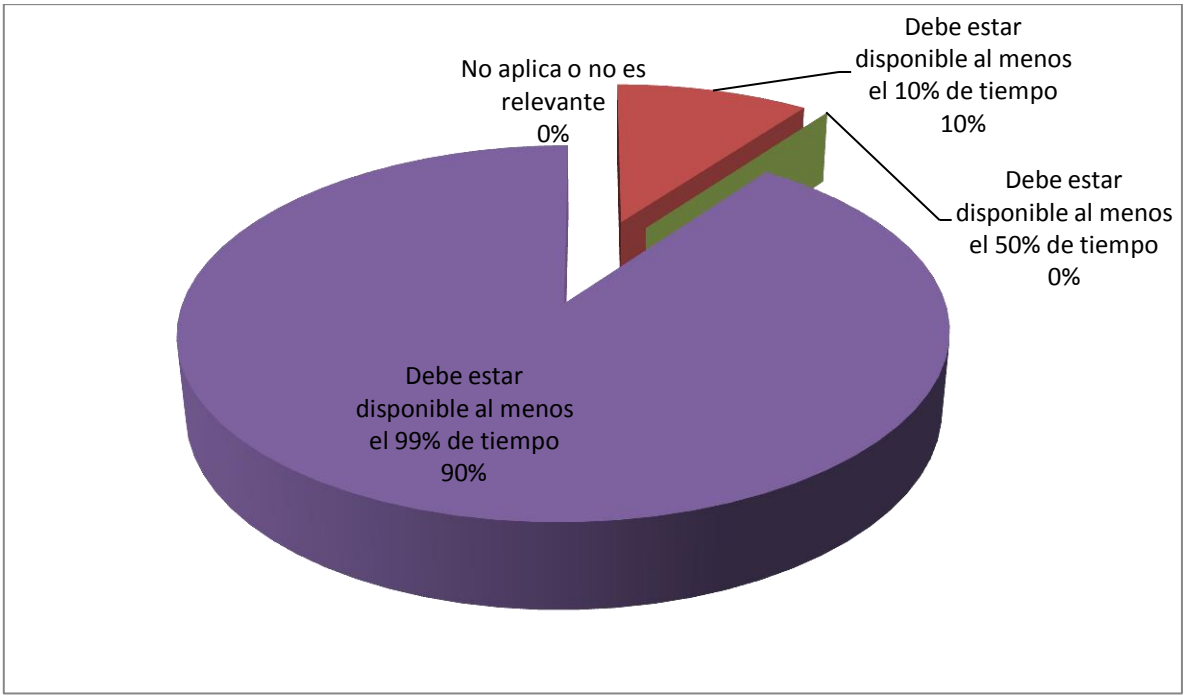


Gráfico: 4.3 Disponibilidad del servicio telefónico (Elaborado por: Investigador)

El 10% considera que debe estar disponible el servicio telefónico en la Institución el 50% del tiempo, mientras que el 90% considera que debe estar disponible al menos el 99% del tiempo.

4.1.1.1.2 Indicador: Confidencialidad

Pregunta: ¿Cuál sería la importancia o el trastorno que tendría que el computador que usted maneja fuera accedido de manera no autorizada?

No aplica o no es relevante	No es relevante los errores que tenga la información faltante	Tiene que estar correcto o completo al menos 95%	Tiene que estar correcto o completo al menos 95%
3	0	0	7

Tabla 4.4: Encuesta dirigida al Personal Docente y Administrativo sobre confidencialidad de equipos (Elaborado por: Investigador)

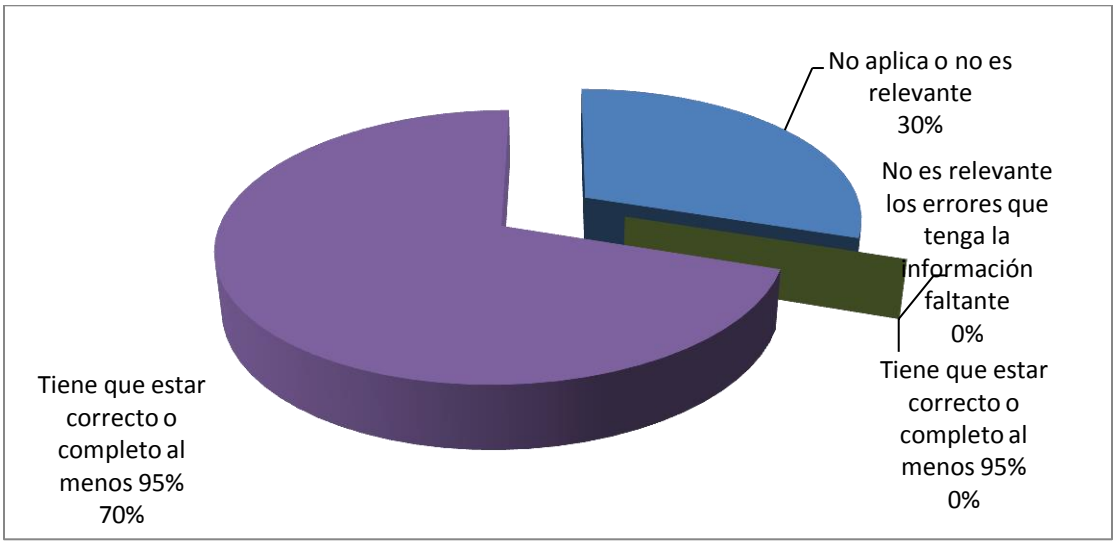


Gráfico: 4.4 Confidencialidad de los equipos (Elaborado por: Investigador)

El 30% considera que no aplica o no es relevante que el computador que maneja fuera accedido de manera no autorizada, el 70% considera que tiene que estar correcto o completo al menos el 95%.

¿Cuál sería la importancia o el trastorno que tendría que las claves de acceso al sistema que le sean entregadas estén en manos de terceros?

No aplica o no es relevante	No es relevante los errores que tenga la información faltante	Tiene que estar correcto o completo al menos 95%	Tiene que estar correcto o completo al menos 95%
0	0	2	8

Tabla 4.5: Tabulación de Encuesta dirigida al Personal Docente y Administrativo sobre confidencialidad de claves de acceso (Elaborado por: Investigador)

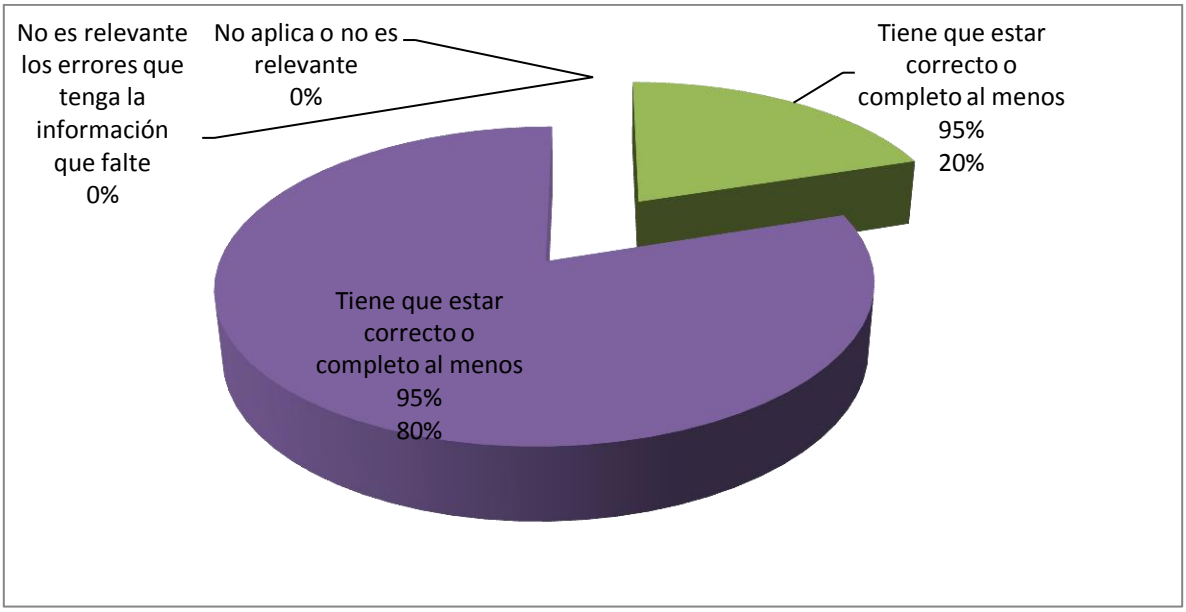


Gráfico: 4.5 Encuesta dirigida al Personal Docente y Administrativo sobre claves de acceso con el indicador confidencialidad (Elaborado por: Investigador)

El 20% considera que las claves de acceso al sistema que le sean entregadas estén en manos de terceros tiene que estar correcto o completo al menos el 50%, el 80% considera que tiene que estar correcto o completo al menos el 95%.

4.1.1.1.3 Indicador: Integridad

Pregunta: ¿Qué importancia tendría que el computador que tiene a su cargo o que está utilizando fuera alterado sin autorización ni control?

No aplica o no es relevante	No es relevante los errores que tenga la información que falte	Tiene que estar correcto o completo al menos50%	Tiene que estar correcto o completo al menos 95%
0	0	0	10

Tabla 4.6 Tabulación encuesta a personal docente sobre la integridad de computadores (Elaborado por: Investigador)

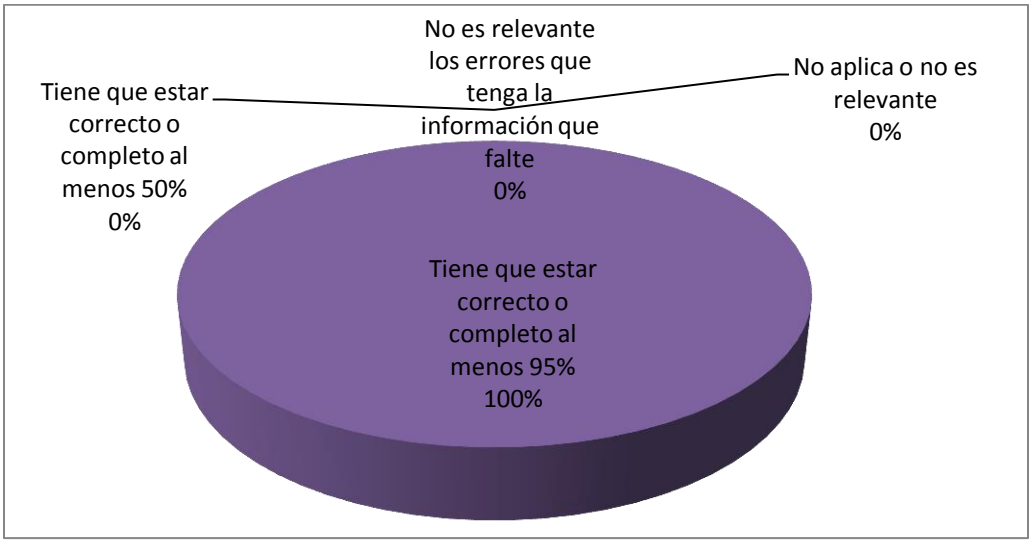


Gráfico: 4.6 Integridad de hardware (Elaborado por: Investigador)

El 100% de los entrevistados manifiesta que el computador que tiene a su cargo tiene que estar correcto o completo al menos el 95%.

4.1.2 Visitas técnicas realizadas al CELP

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

MAESTRÍA EN REDES Y TELECOMUNICACIONES

GUÍA DE VISITA TÉCNICA REALIZADA EN EL CENTRO EDUCATIVO LA PRADERA

Objetivo: Obtener información de la dimensión software del CELP.

Fecha: 1/oct/2013 al 18/oct/2013 **Nombre:** Ing. Tannia Mayorga

Hora de inicio: 8h00 **Hora de finalización:** 12h00

Responsables de la visita: Arq. Luis Atapuma, Lic. David De La Cruz, Lic. Viviana Sanguano.

Actividades realizadas

4.1.2.1 **Dimensión hardware**

4.1.2.1.1 Indicador: Espacio físico

- Revisión de las instalaciones físicas donde se encuentra el hardware del CELP.

Observación:

El lugar donde se encuentran los equipos del Laboratorio de Tics tiene humedad, la puerta de acceso no tiene ventana, no existen suficientes tomas eléctricas, hay cables en el piso, la ubicación de los equipos que utilizan los estudiantes, no permite ver qué es lo que hacen, pues el equipo que utiliza el docente está al lado de la puerta, no hay mucho espacio para caminar (Ver anexo 9).

Los equipos del área Administrativa, se encuentran ubicados de una manera adecuada.

4.1.2.1.2 Indicador: Tecnología

- Obtener información de los activos de hardware.

Observación:

El Laboratorio de Tics está formado por 15 equipos cuyas características no se describen por seguridad, disponen de un router, 2 switch, 1 servidor de aplicaciones, equipos del área administrativa.

4.1.2.2 Dimensión software

4.1.2.2.1 Indicador: Educativo

- Revisión del software educativo instalado en los computadores del Laboratorio de Tics.

Observación:

El software educativo que tienen es: Inglés Grancaco, Matemáticas, Software para prebásica, juegos.

4.1.2.2.2 Indicador: Licencias

Observación:

El CELP dispone de licencias del Sistema Operativo del Servidor de aplicaciones, no dispone de licencias de software del Laboratorio de Tics.

4.1.2.2.3 Indicador: Tipo

- Revisión del tipo de software instalado en el CELP

Observación:

El tipo de software que tiene instalado en el Laboratorio de Tics, y área administrativa es propietario (Windows, Microsoft Office), el software de la base de datos es My sql, libre, al igual que el navegador Firefox, java, ruby.

4.1.2.2.4 Indicador: Calidad

- El sistema de gestión de información es de fácil manejo.
- El tiempo de respuesta es adecuado en el procesamiento de la información.
- Tiene que ver con la formación el uso del sistema de gestión de información del CELP.

Observación:

Se observa que el sistema de gestión de información maneja una arquitectura de 3 capas, sus interfaces son amigables, de fácil manejo.

El tiempo de respuesta no es adecuado ya que se demoraba en ingresar la secretaria 15 minutos.

El sistema cuenta con un módulo para que el personal docente pueda publicar en Internet las tareas que los estudiantes requieren realizar para el siguiente día, a las que los padres de familia pueden tener acceso.

El sistema se encuentra en la fase de paso a producción, y presenta errores de forma y otras correcciones que tienen que hacer para enlazar con la página web del CELP.

La página web del CELP se encuentra ubicada en un hosting en EEUU, no se encuentra actualizada y se observan errores en ciertas opciones.

4.1.2.2.5 Indicador: Seguridad

- Observar si los equipos del CELP tienen instalado un antivirus.
- Constatar la periodicidad de actualización del antivirus en el CELP.
- Ver si tienen software que mejore la seguridad informática.

Observación:

El antivirus instalado en los equipos del CELP es el Avast, no se actualiza porque tienen instalado el software Deep Freeze, y únicamente el Propietario es el que maneja la clave.

El software de seguridad es el Deep Freeze.

El servidor de archivos tiene instalado Windows 7.

El software squid para compartir Internet en el Laboratorio de Tics sin configurar adecuadamente.

4.1.2.3 **Dimensión red**

- Observar si existe confiabilidad, integridad, disponibilidad de la red

4.1.2.3.1 Confiabilidad

Observación:

La red no es confiable ya que no se encuentra bien configurada, las interfaces de red, tienen grupos de trabajo diferentes, direcciones IP sin secuencia, no existe políticas de direccionamiento IP, por lo que se presentan conflictos de direccionamiento IP. No existe un servidor con un sistema operativo de red.

La red no está integrada, tienen 2 segmentos de red, el del área administrativa y el del Laboratorio de Tics, que es una red Wireless; el área administrativa comparte Internet con el switch, y el Laboratorio de Tics comparte Internet con squid, que se encuentra únicamente configurado para compartir sin seguridad alguna.

Los equipos de comunicaciones se encuentran conectados directamente a tomas corrientes, al igual que el servidor de archivos.

4.1.2.3.2 Integridad

Observación:

La información de registro de estudiantes ingresada en secretaría no se guarda, lo que evidencia una mala configuración en la red ya que se demora 15 minutos en abrir el sistema o realizar cualquier actualización con el servidor de archivos.

La red no tiene algún mecanismo de autenticación.

4.1.2.3.3 Disponibilidad

Observación:

La red se encuentra disponible únicamente cuando el Propietario de la Institución enciende los equipos de comunicaciones que se encuentra en su oficina.

El servidor de Aplicaciones también se encuentra ubicado en la oficina del Propietario por lo que existe el mismo inconveniente que con los equipos de comunicaciones.

4.1.3 Entrevista dirigida a la jefatura de talento humano

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

MAESTRÍA EN REDES Y TELECOMUNICACIONES

ENREVISTA DIRIGIDA A LA JEFATURA DE TALENTO HUMANO DEL CENTRO EDUCATIVO LA PRADERA

Objetivo: Indagar sobre las responsabilidades, roles del personal docente y administrativo en lo que respecta a la seguridad informática

Pregunta	Respuesta
¿Tiene definido políticas, roles y responsabilidades de seguridad informática de los empleados, estudiantes, padres de familia, terceros?	Si, cada quien sabe qué es lo que tiene que hacer en la Institución, pero de seguridad informática no.
¿Tienen establecido en el contrato de trabajo el personal los roles y responsabilidades y las de la organización para la seguridad de información?	No está establecido

Tabla 4.7: Entrevista a Jefe de Talento Humano sobre responsabilidades y roles del personal docente y administrativo de seguridad informática (Elaborado por: Investigador)

Objetivo: Indagar si el elemento humano está al tanto sobre amenazas, inquietudes sobre la seguridad de la información

Pregunta	Respuesta
¿Tienen definidas políticas y procedimientos en donde se garantice la aplicación de Gestión de Responsabilidades?	Los padres de familia firman un documento en el que constan varias responsabilidades, en secretaría está el documento donde puede revisarle, del resto no.
¿Reciben los empleados capacitaciones en lo que respecta a seguridad de la información?	No reciben
¿Existe algún proceso disciplinario cuando algún empleado ha cometido alguna violación en la seguridad?	Lo estipulado en el código de convivencia que tienen en secretaría, pero están por elaborar otro nuevo en base a las nuevas leyes.
¿Están claramente definidas las responsabilidades a la terminación o cambio de empleo en cuanto a seguridad de información?	No está claro
¿Los empleados devuelven todos los activos al terminar sus funciones?	Si
¿Cuál es el proceso de eliminación de derechos de acceso cuando un empleado termina sus funciones?	No está establecido

Tabla 4.8: Entrevista realizada a Jefe de Talento Humano sobre amenazas de seguridad informática (Elaborado por: Investigador)

4.1.4 Entrevista dirigida al encargado de tecnología y propietario usando los indicadores: respaldos, control de acceso.

4.1.4.1 **Dimensión: información**

4.1.4.1.1 Indicador: respaldos

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

MAESTRÍA EN REDES Y TELECOMUNICACIONES

ENTREVISTA DIRIGIDA AL ENCARGADO DE TECNOLOGÍA Y PROPIETARIO DEL CENTRO EDUCATIVO LA PRADERA

Objetivo: Indagar sobre el manejo de respaldos de la información

Pregunta	Respuesta Encargado de Tecnología	Respuesta Propietario
¿Quién respalda la información?	No existe nadie preparado	La secretaria
¿Realizan copias de seguridad de la información en forma periódica?	La secretaria debería hacerlo	No lo se
¿Existen definidos procedimientos para realizar copias de seguridad de la información?	No existen	No existen
¿Existe un lugar seguro fuera de la institución donde permanezca una copia de los respaldos de la información?	No está definido	No
¿Cuenta la institución con un plan de contingencia ante recuperación de desastres?	No lo se	El Institucional

Tabla 4.9: Entrevista dirigida al Encargado de Tecnología y Propietario sobre manejo de respaldos de la información (Elaborado por: Investigador)

4.1.5 Entrevista dirigida al encargado de tecnología, desarrollador y propietario sobre: Sistema de Gestión de Información y Base de Datos

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

MAESTRÍA EN REDES Y TELECOMUNICACIONES

Entrevista dirigida al Encargado de tecnología, Desarrollador del Sistema y Propietario del CENTRO EDUCATIVO LA PRADERA

Objetivo: Indagar sobre las seguridades que tiene el Sistema de Gestión de Información y la Base de datos

4.1.5.1 **Dimensión Software**

4.1.5.1.1 Indicador Sistema de Gestión de Información – Información (Base de datos)

Pregunta	Resp. Encargado de Tecnología	Resp. Desarrollador	Resp. Propietario
¿Existen políticas para la asignación de usuarios y perfiles de acceso?	**No**	El sistema está en proceso de implementación	Tiene que entregarme el manual
¿Están las contraseñas almacenadas usando algún método de encriptación?	**Si**	**Si**	Eso sabe el Encargado de Tecnología
¿Existe políticas que aseguren el acceso a la información a la Base de Datos?	**No**	**No**	Eso sabe el Encargado de Tecnología

Tabla 4.10: Entrevista dirigida al encargado de tecnología, desarrollador y propietario sobre el Sistema de Gestión de la Información y Base de Datos (Elaborado por: Investigador)

4.1.6 Encuesta dirigida al Personal docente usando los indicadores: Internet, Tics, Herramientas de búsqueda guiada.

4.1.6.1 Dimensión: recursos tecnológicos

4.1.6.1.1 Indicador: Internet - peligros

Pregunta: Cuando usted usa el Internet para dar sus clases, ¿cree que pueden los alumnos estar expuestos a peligros tecnológicos?

Si	No	A veces	Tal vez	No se
6	1	0	0	0

Tabla: 4.11 Tabulación encuesta dirigida al personal docente sobre exposición de alumn@s a peligros de Internet (Elaborado por: Investigador)

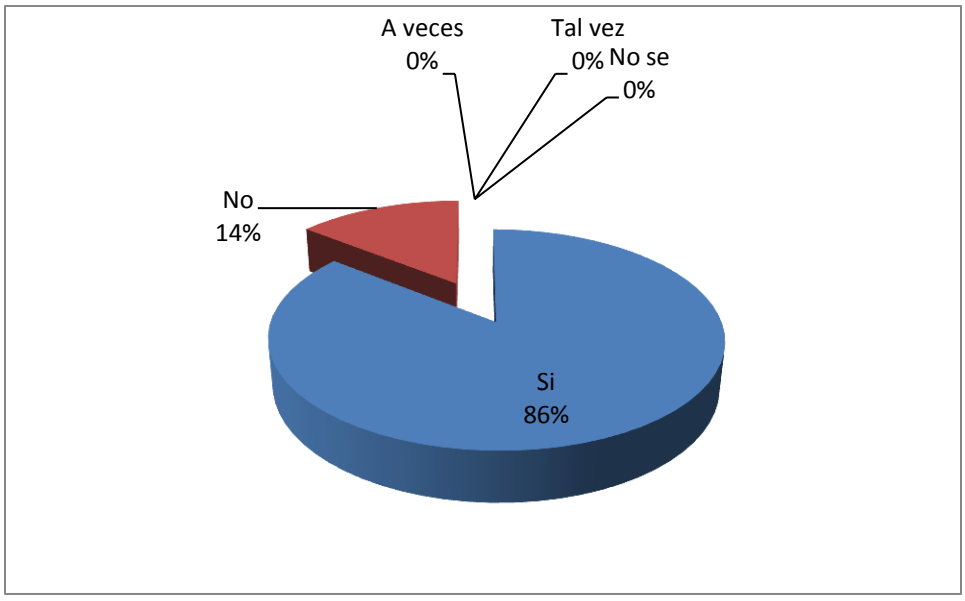


Gráfico: 4.7 Exposición de alumn@s a peligros de Internet (Elaborado por: Investigador)

El 86% de Docentes cuando utilizan Internet para dar sus clases, considera que los niños, niñas y adolescentes si pueden estar expuestos a los peligros de Internet, el 14 % considera que no.

4.1.6.1.2 Indicador Tics

Pregunta: ¿Usted utiliza Software educativo para dictar sus clases?

Si	No
3	4

Tabla 4.12: Tabulación de encuesta dirigida al Personal Docente sobre uso de software educativo (Elaborado por: Investigador)

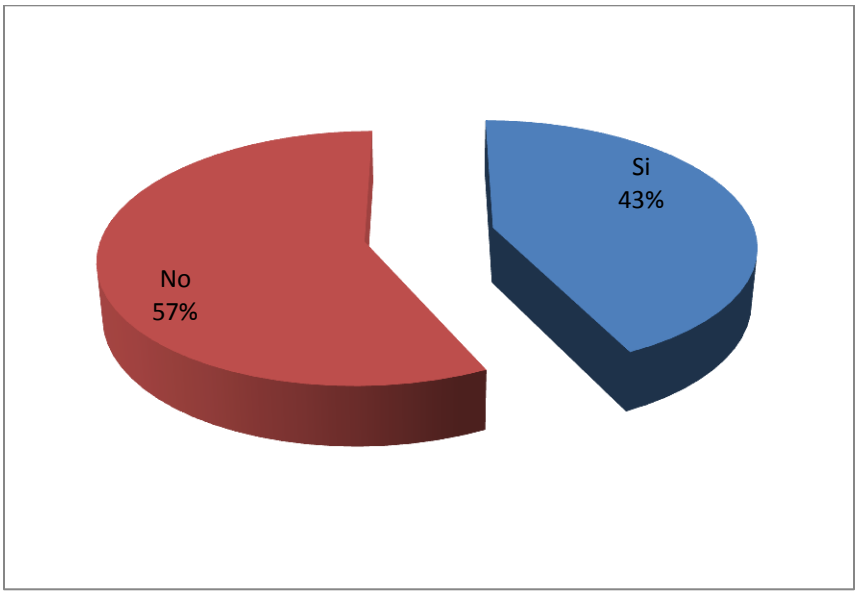


Gráfico: 4.7 Uso de los docentes de software educativo (Elaborado por: Investigador)

El 43% dice Si utiliza software educativo para dictar sus clases, el 57,14% dice Si cree que los recursos tecnológicos con que cuenta la Institución son adecuados para utilizarlos como herramienta de apoyo en la formación de los alumnos., el 28,57%.

Pregunta: ¿Cree usted que los recursos tecnológicos con que cuenta la Institución son adecuados para utilizarlos como herramienta de apoyo en la formación de los estudiantes?

Si	No	Tal vez
4	2	1

Tabla 4.13: Tabulación de encuesta dirigida al Personal Docente sobre recursos tecnológicos son adecuados para ser usados como herramienta de apoyo en la formación de los estudiantes (Elaborado por: Investigador)

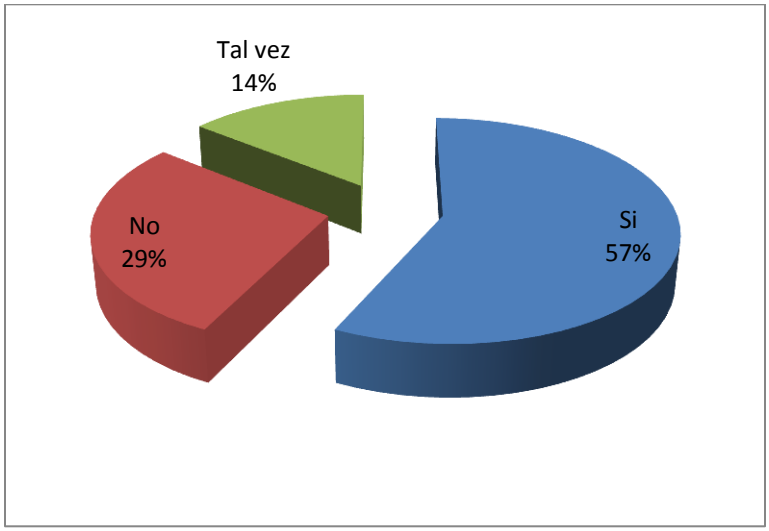


Gráfico: 4.8 Recursos tecnológicos son adecuados para ser usados como herramienta de apoyo en la formación de los estudiantes (Elaborado por: Investigador)

El 14% del personal docente que los recursos tecnológicos tal vez son adecuados para ser usados como herramienta de apoyo en la formación de los estudiantes del CELP; el 29% manifiesta que no son adecuados para ser usados como herramienta de apoyo en la formación de los estudiantes; el 57% manifiesta que si son adecuados para ser usados como herramienta de apoyo en la formación de los estudiantes.

Pregunta: ¿Considera que las Tics son de ayuda para la educación de los estudiantes del CELP?

Si	No	Tal vez
7	0	0

Tabla 4.14: Tabulación de encuesta dirigida al Personal Docente sobre si las Tic son de ayuda para la educación de los estudiantes del CELP (Elaborado por: Investigador)

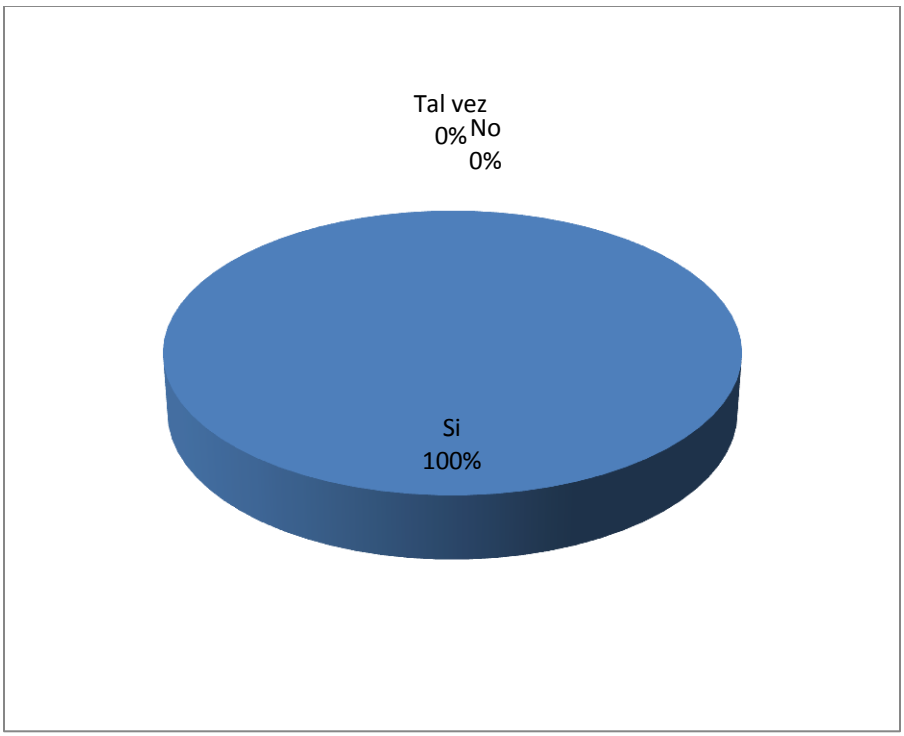


Gráfico: 4.9 Tics son de ayuda para la educación de los estudiantes del CELP (Elaborado por: Investigador)

El 100% del personal docente manifiesta que las Tics son de ayuda para la educación de los estudiantes del CELP.

Pregunta: ¿Le gustaría que le capaciten en el uso de herramientas orientadas a las Tics en el Internet?

Si	No	Tal vez
7	0	0

Tabla 4.15: Tabulación de encuesta dirigida al Personal Docente sobre capacitación de herramientas Tics en el Internet (Elaborado por: Investigador)

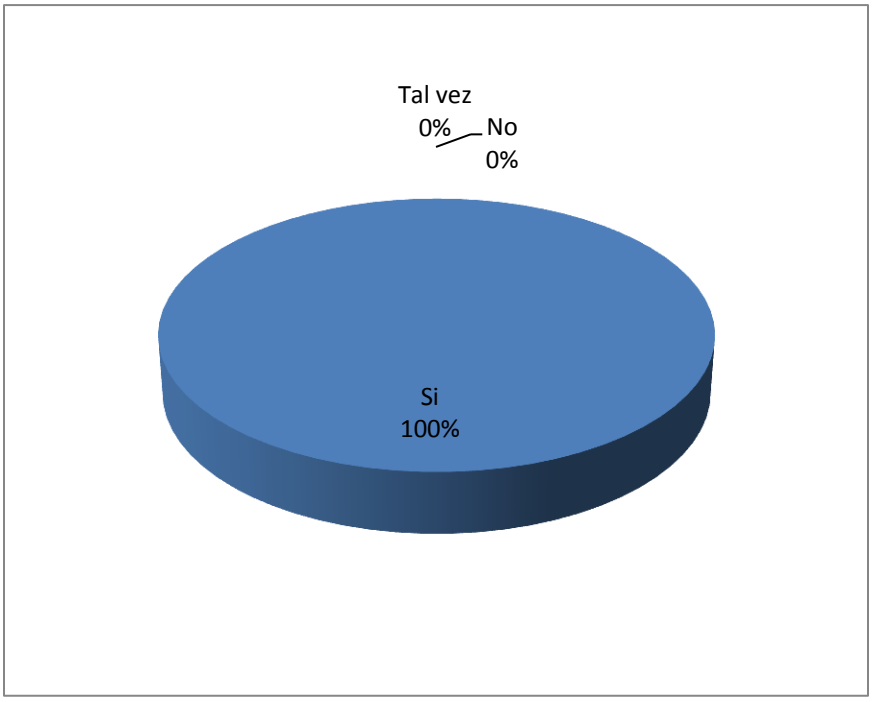


Gráfico: 4.10 Tabulación de Encuestas dirigida a los Docentes sobre TIC (Elaborado por: Investigador)

El 100% del personal docente manifiesta que si es necesario capacitar a los profesores en herramientas Tic.

Pregunta: ¿Sabe lo que son webquest y caza de tesoro?

Si	No	Tal vez
0	7	0

Tabla 4.16: Tabulación de encuesta dirigida al Personal Docente sobre si saben lo que son: webquest y caza de tesoro (Elaborado por: Investigador)

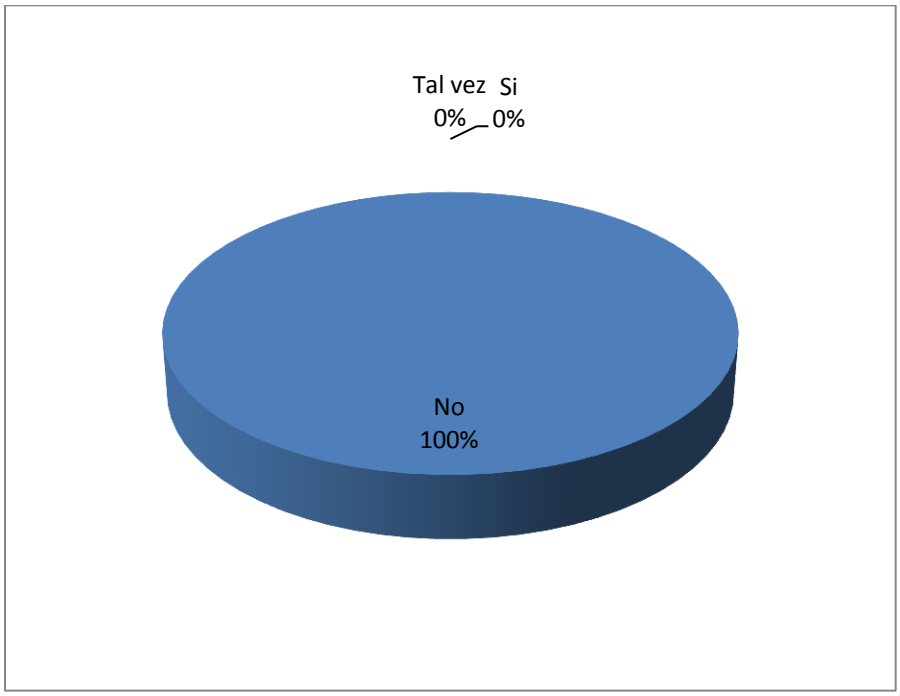


Gráfico: 4.11 Tabulación de Encuestas dirigida a los Docentes sobre uso de webquest y caza de tesoro (Elaborado por: Investigador)

El 100% de los Docentes no sabe que es webquest o caza de tesoro.

4.1.7 Entrevista realizada al Encargado de Tecnología y Propietario sobre Control de acceso a Internet

4.1.7.1 **Dimensión recursos tecnológicos**

4.1.7.1.1 Indicador: Internet – control de acceso

Objetivo: Indagar sobre el control de acceso

Pregunta	**Resp.** **Encargado de Tecnología**	**Resp.** **Propietario**
¿Los docentes tienen acceso a la red, y al uso de Internet?	Si, el computador que se encuentra en el DOBE, lo único que falta es formatearle e instalar WinXP	Pueden acceder en el equipo del DOBE y en Inspección
¿Existen políticas que permitan hacer un uso adecuado de la red?	No	No
¿Existen bitácoras del control de uso de Internet?	No se	No se
¿Existe algún proceso para que un docente utilice el laboratorio Tics?	No se	Tienen que solicitar
¿Existe algún procedimiento para autorización de ingreso o salida de equipos fuera del laboratorio de TICs o de la Institución?	Debe autorizar el dueño	Yo autorizo
¿Tiene algún mecanismo que permita compartir internet de manera segura?	No	No se

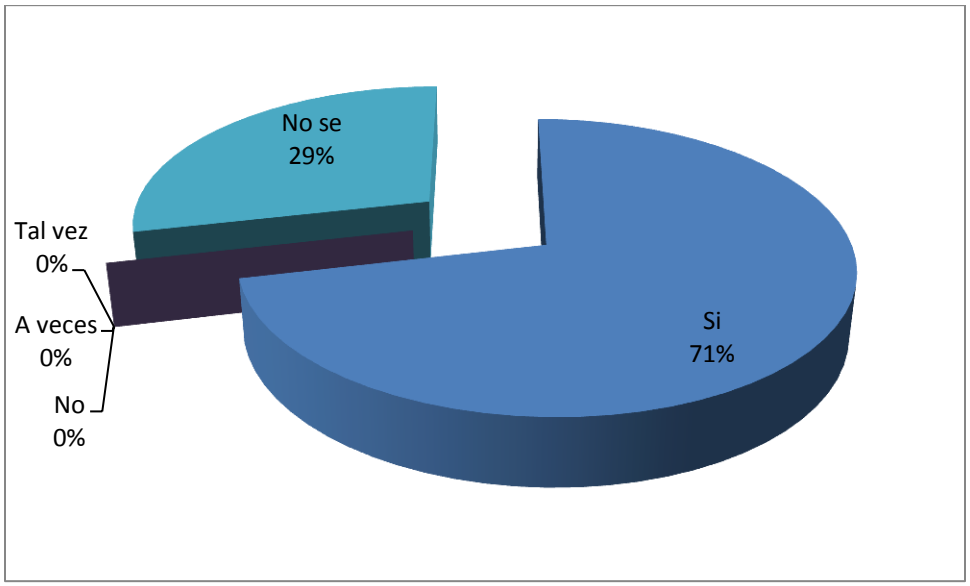
Tabla 4.17: Entrevista realizada al Encargado de Tecnología y Propietario sobre el Control de Acceso a internet (Elaborado por: Investigador)

4.1.7.1.2 Indicador: Tics

Pregunta: ¿Considera usted que el Internet ayudaría a la formación académica de los estudiantes?

Si	No	A veces	Tal vez	No se
5	0	0	0	2

Tabla 4.18: Tabulación de encuesta dirigida al personal docente sobre si el Internet ayudaría a la formación académica de los estudiantes (Elaborado por: Investigador)



Gráfica 4.12 Internet ayudaría a la formación académica de los estudiantes (Elaborado por: Investigador)

El 29% no sabe si ayudaría el Internet a la formación académica de los estudiantes, el 71% considera que el Internet si ayudaría a la formación académica de los estudiantes.

Pregunta: ¿Existe en la institución alguna política, norma, estándar o procedimiento para solicitar el uso de Internet?

Si	No	A veces	Tal vez	No se
5	0	0	0	2

Tabla 4.19 Tabulación encuesta dirigida al personal docente sobre la existencia de políticas, normas, estándar o procedimiento para solicitar el uso de Internet (Elaborado por: Investigador)

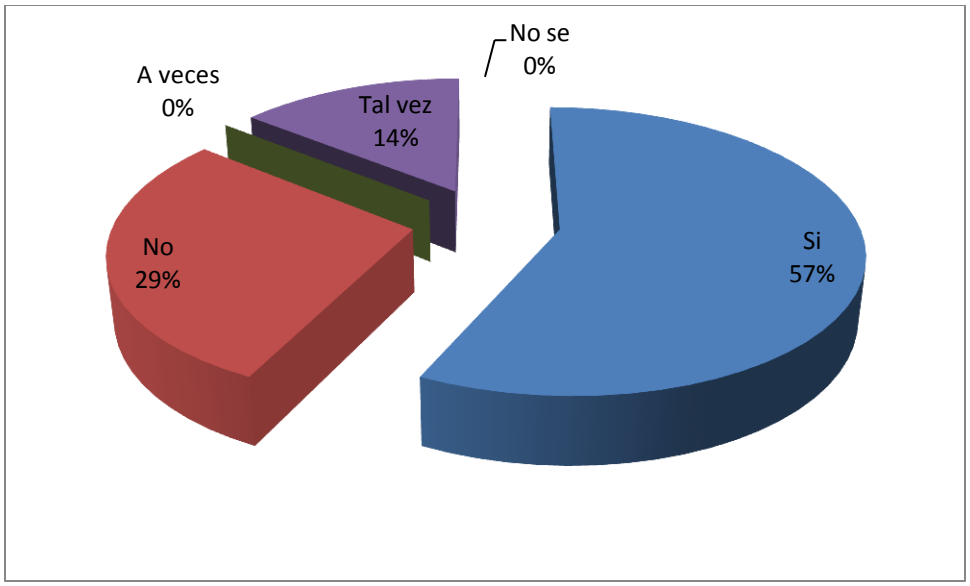


Gráfico: 4.13 Existencia de alguna política, norma, estándar o procedimiento para solicitar el uso de Internet (Elaborado por: Investigador)

El 57% de Docentes dice que si existen políticas, estándar o procedimiento para solicitar el uso de Internet, el 29% dice que no, el 14% dice tal vez.

4.1.7.2 **Dimensión: Herramientas de apoyo**

4.1.7.2.1 Indicador: Herramienta de búsqueda guiada

Pregunta: Cuando usted usa el Internet ¿tiene la precaución de dirigir la consulta o investigación a sitios seguros?

Si	No	A veces	Tal vez	No se
2	4	0	0	1

Tabla 4.20: Tabulación de encuesta dirigida al personal docente sobre dirigir las investigaciones en Internet a sitios seguros (Elaborado por: Investigador)

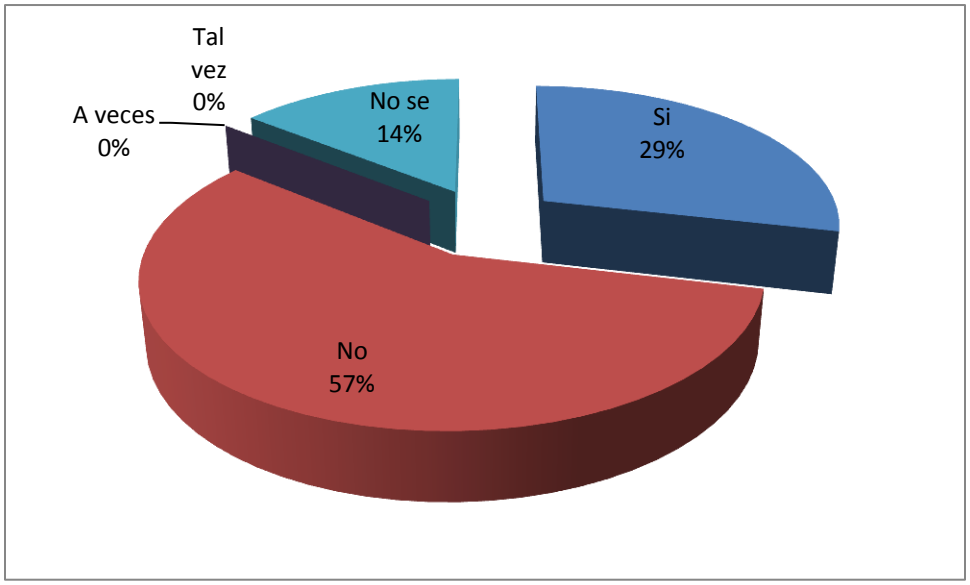


Gráfico: 4.14 Docentes dirigen las investigaciones de sus estudiantes en Internet a sitios seguros (Elaborado por: Investigador)

El 57% de Docentes no dirige las investigaciones a sitios seguros, el 29% si, dirige sus Investigaciones a sitios seguros y el 14,29% no sabe, lo que significa que el 71% de docentes no dirige o no sabe cómo dirigir las investigaciones de Internet a sitios seguros.

4.1.7.2.2 Indicador: Equipos de tecnología

Pregunta: ¿Dispone de un computador para realizar sus investigaciones en internet en el CELP?

Si	No	Tal vez
1	6	0

Tabla 4.21 Tabulación encuesta realizada al personal docente sobre si dispone de un computador para realizar sus investigaciones en internet en el CELP

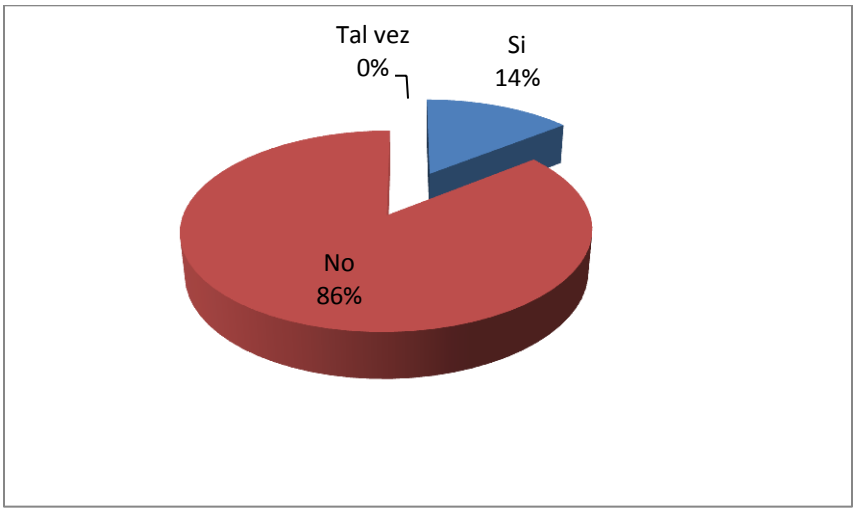


Gráfico: 4.15 Uso de equipos con Internet en el CELP para investigaciones (Elaborado por: Investigador)

El 42,86% dice que si dispone de un computador para realizar sus investigaciones en Internet en el CELP, el 50% dice tal vez y el 92,86% dice no saber.

Pregunta: ¿Existe alguna política, norma, estándar o procedimiento para solicitar el uso de Laboratorio para dictar sus clases?

Si	No	Tal vez
2	4	1

Tabla 4.22 Tabulación de encuesta realizada al personal docente sobre la existencia de alguna política, norma, estándar o procedimiento para solicitar el laboratorio para dictar sus clases (Elaborado por: Investigador)

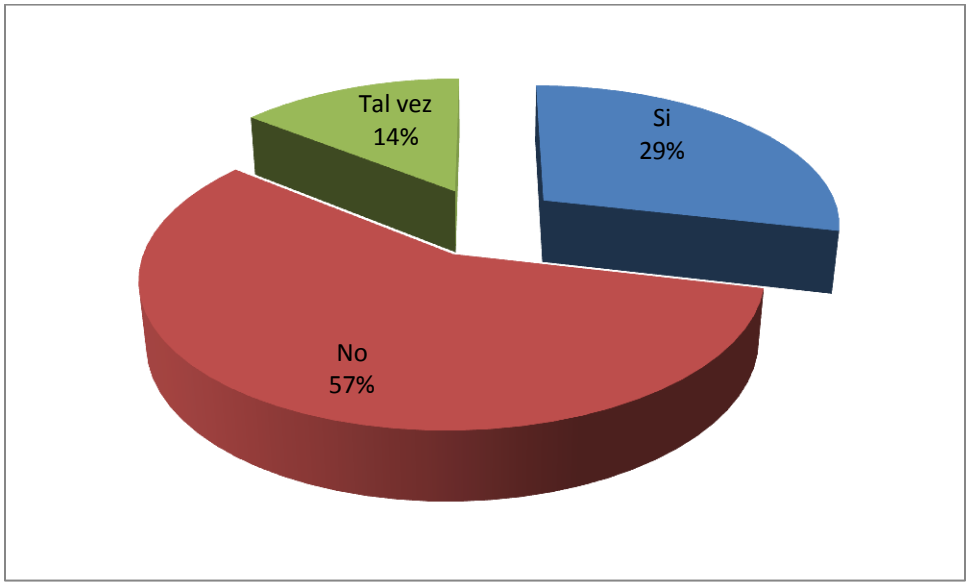


Gráfico: 4.16 Existencia de alguna política, norma, procedimiento para solicitar el laboratorio para dictar clases (Elaborado por: Investigador)

El 33,33 % dice que si existe alguna política, norma, procedimiento para solicitar el uso del Laboratorio para dar sus clases, el 8,33% dice no y el 58,33% dice tal vez.

Pregunta: ¿Tiene conocimiento si existe alguna política, norma, estándar o procedimiento para garantizar seguridad informática en el CELP?

Si	No	Tal vez
1	5	1

Tabla 4.23: Encuesta dirigida al Personal docente sobre la existencia de alguna política, norma, procedimiento o estándar para garantizar la seguridad informática en el CELP (Elaborado por: Investigador)

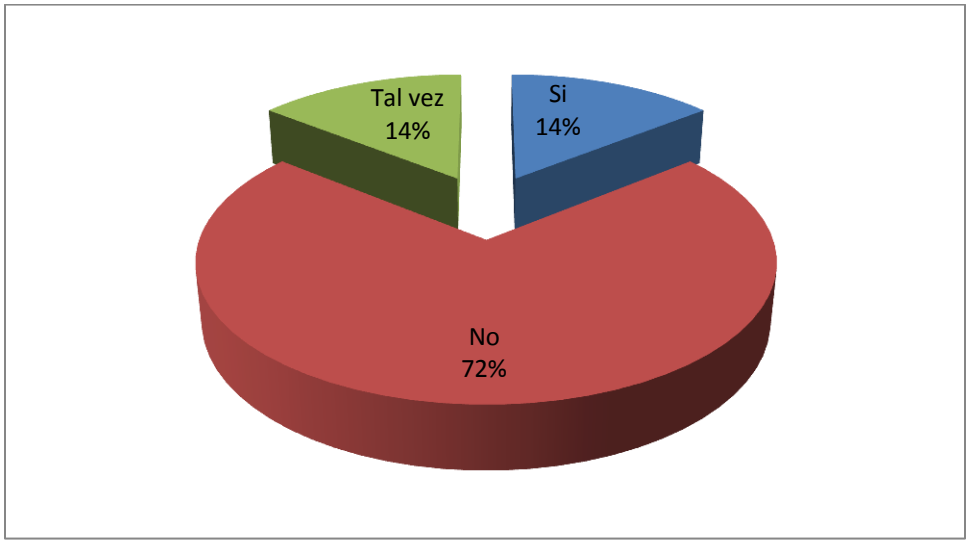


Gráfico: 4.17 Existencia de alguna política, norma, procedimiento, estándar para garantizar la seguridad informática en el CELP (Elaborado por: Investigador)

El 14% dice que si existe alguna política, norma, procedimiento, estándar para garantizar la seguridad informática en el CELP", el 14% dice tal vez exista, el 72% dice que no existe.

4.1.8 Encuesta dirigida a estudiantes del CELP

4.1.8.1 Indicador: Internet – Peligros

Pregunta: ¿Sabe lo que es pornografía?

Si	No	Tal vez
13	13	0

Tabla 4.24: Tabulación de Encuesta realizada a los estudiantes sobre si conocen lo que es pornografía (Elaborado por: Investigador)

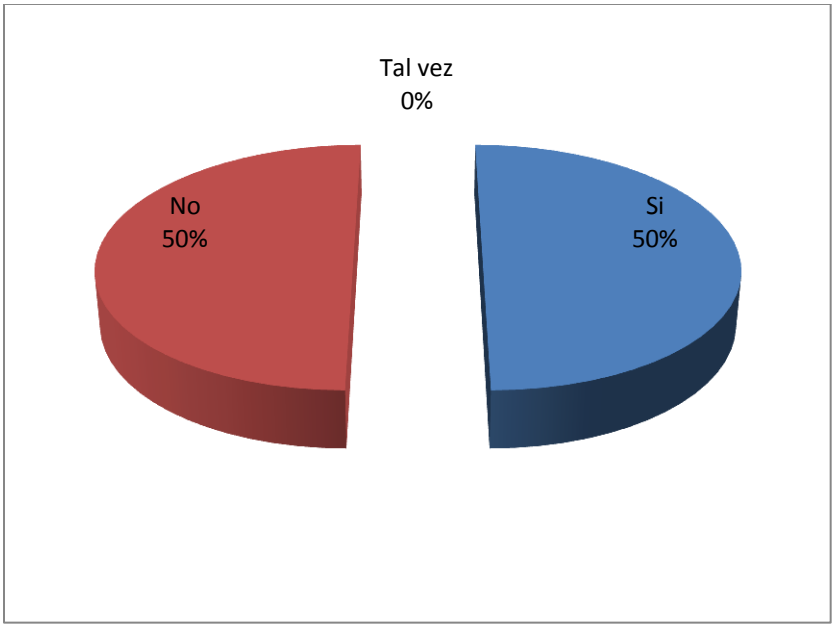


Gráfico: 4.18 Conocimiento de pornografía de los estudiantes del CELP (Elaborado por: Investigador)

El 50% de los estudiantes si sabe lo que es pornografía, el 50 % no sabe.

Pregunta: ¿Ha visto pornografía en Internet?

Si	No	Tal vez
9	16	1

Tabla 4.25: Tabulación de Encuesta realizada a los estudiantes sobre si han visto pornografía en Internet (Elaborado por: Investigador)

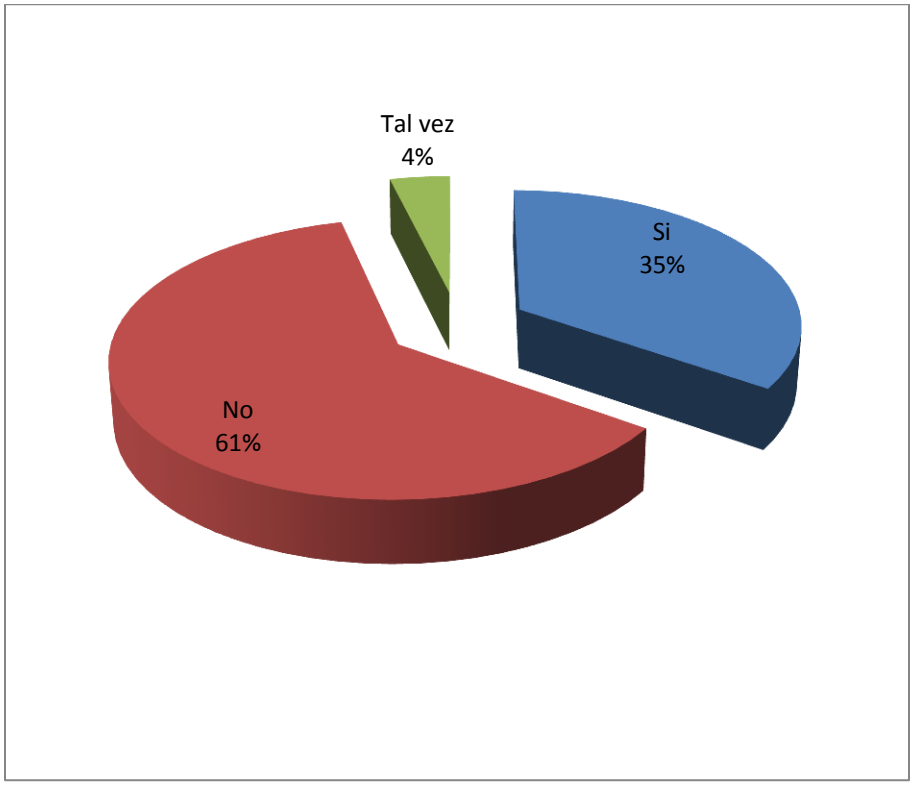


Gráfico: 4.19 Pornografía vista en Internet por los estudiantes del CELP (Elaborado por: Investigador)

El 35 % de los estudiantes si han visto pornografía en Internet, el 61% no ha visto pornografía en Internet y el 4% tal vez ha visto pornografía en Internet.

Pregunta: ¿Ha tenido acceso a pornografía en forma accidental?

Si	No	Tal vez
10	17	0

Tabla 4.26: Tabulación de Encuesta realizada a los estudiantes sobre si han tenido acceso a pornografía en Internet en forma accidental (Elaborado por: Investigador)

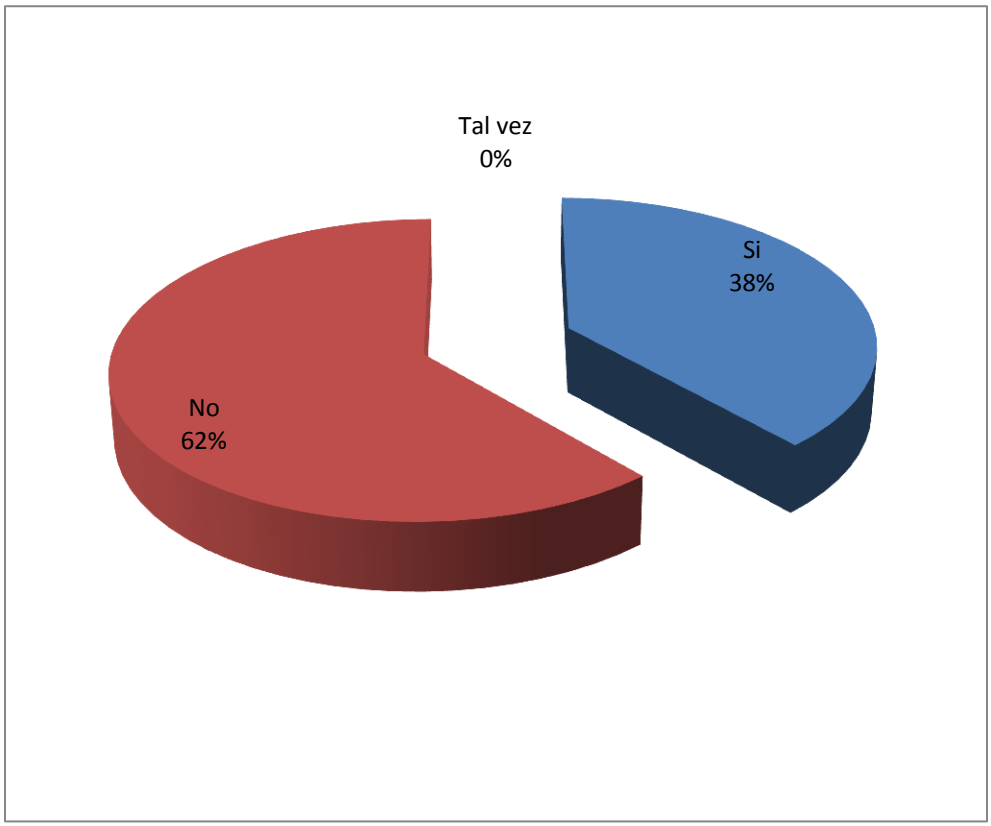


Gráfico: 4.20: Acceso a pornografía en forma accidental de los estudiantes del CELP (Elaborado por: Investigador)

El 38 % de los estudiantes ha tenido acceso a pornografía en forma accidental, el 62% no ha tenido acceso a internet en forma accidental.

Pregunta: ¿Ha tenido propuestas inadecuadas en Internet por desconocidos?

Si	No	Tal vez
8	17	2

Tabla 4.27: Tabulación de Encuesta realizada a los estudiantes sobre si han tenido propuestas inadecuadas en Internet por desconocidos (Elaborado por: Investigador)

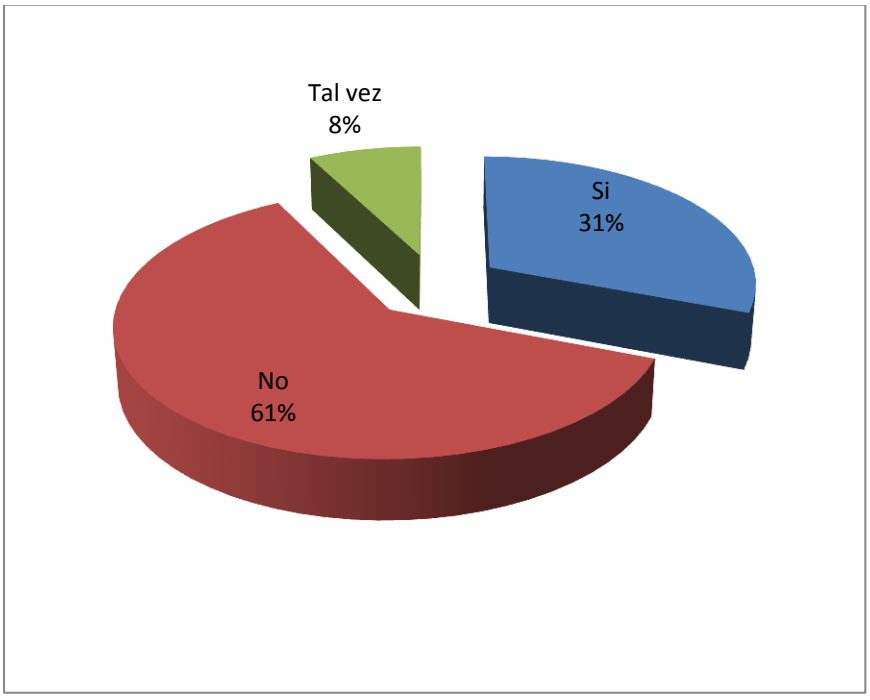


Gráfico: 4.21 Propuestas inadecuadas en Internet por desconocidos a estudiantes del CELP (Elaborado por: Investigador)

El 31 % de estudiantes Si ha tenido propuestas inadecuadas en Internet, el 61 % de los estudiantes no ha tenido propuestas inadecuadas en Internet y el 8 % de los estudiantes tal vez ha tenido propuestas inadecuadas en Internet.

Pregunta: ¿Sabe lo que es cyberbulling?

Si	No	Tal vez
0	27	0

Tabla 4.28: Tabulación de Encuesta realizada a los estudiantes sobre si saben lo que es cyberbulling (Elaborado por: Investigador)

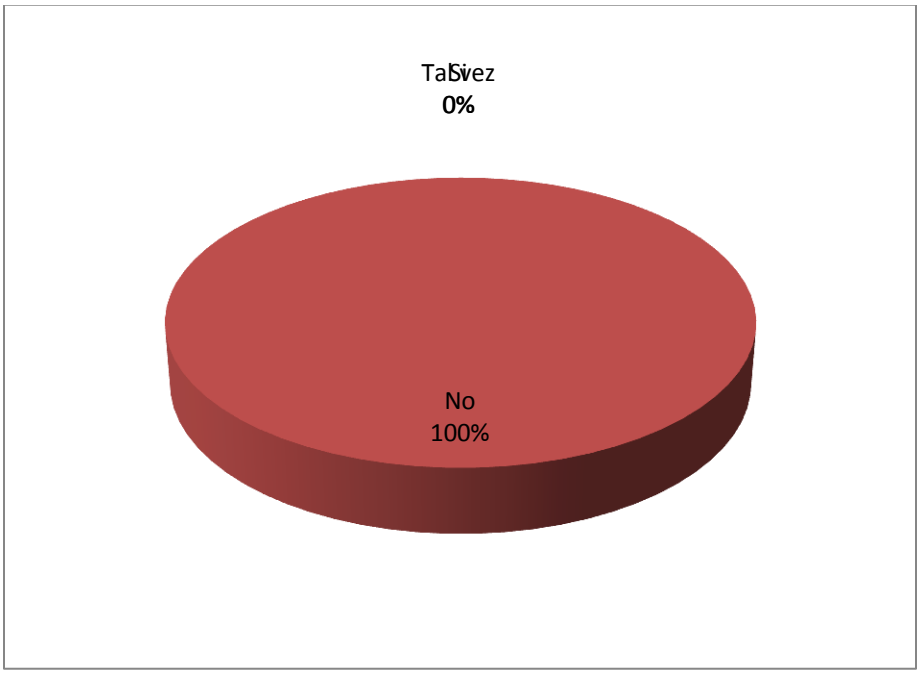


Gráfico: 4.22 Conocimiento del significado de cyberbulling de los estudiantes del CELP (Elaborado por: Investigador)

El 100% de los estudiantes no saben lo que es cyberbulling.

Pregunta: ¿Ha sido víctima de algún engaño en Internet?

Si	No	Tal vez
4	23	0

Tabla 4.29: Tabulación de Encuesta realizada a estudiantes sobre si han sido víctimas de algún engaño en Internet (Elaborado por: Investigador)

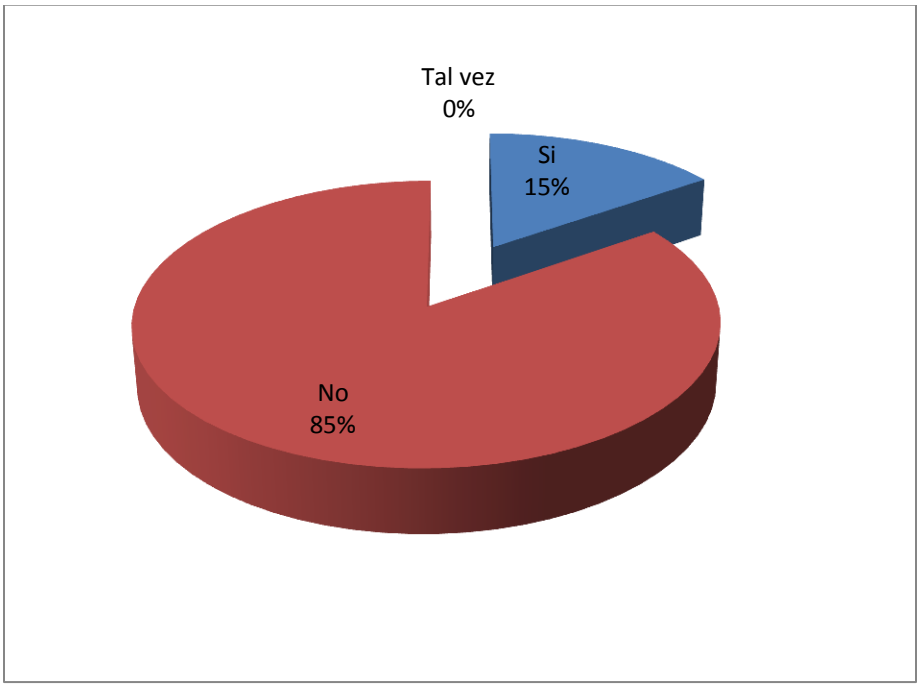


Gráfico: 4.23 Víctimas de algún engaño en Internet en los estudiantes del CELP (Elaborado por: Investigador)

El 15% de los estudiantes si ha sido víctima de algún engaño en Internet, el 85% no ha sido víctima de algún engaño en Internet.

Pregunta: Cuando a usted le aparece en Internet alguna imagen inadecuada a su edad ¿qué hace?

Opciones	**Frecuencia**
Le avisa a sus padres	4
Le cuenta a un adulto	5
Comenta con un profesor	1
Comenta con algún compañero	4
Se queda callado	12
	26

Tabla 4.30: Tabulación sobre lo que hacen los estudiantes del CELP, cuando le aparece en Internet alguna imagen inadecuada a su edad (Elaborado por: Investigador)

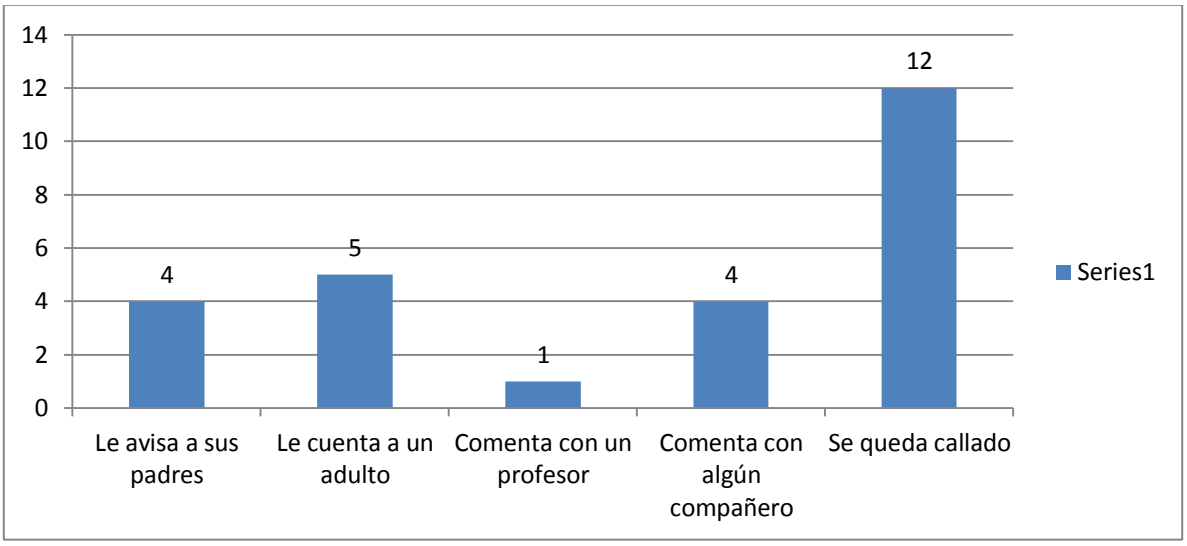


Gráfico: 4.24 Lo que hacen los estudiantes del CELP cuando les aparece alguna imagen inadecuada a su edad (Elaborado por: Investigador)

De una muestra de 26 estudiantes el 15,38% les avisa a sus padres cuando le aparece en Internet alguna imagen inadecuada a su edad, el 19,23 % le cuenta a un adulto, el 3,85% le comenta a un profesor, el 15,38 % comenta con algún compañero, y el 46,15% se queda callado.

4.1.9 Encuesta dirigida a padres de familia

4.1.9.1 Indicador: Internet – peligros

Pregunta: ¿Sabe si su hijo(a) sabe lo que es pornografía?

Si	No	Tal vez
8	6	1

Tabla 4.31: Tabulación encuesta dirigida a los padres de familia, donde expresan si conocen sus hij@s que es pornografía (Elaborado por: Investigador).

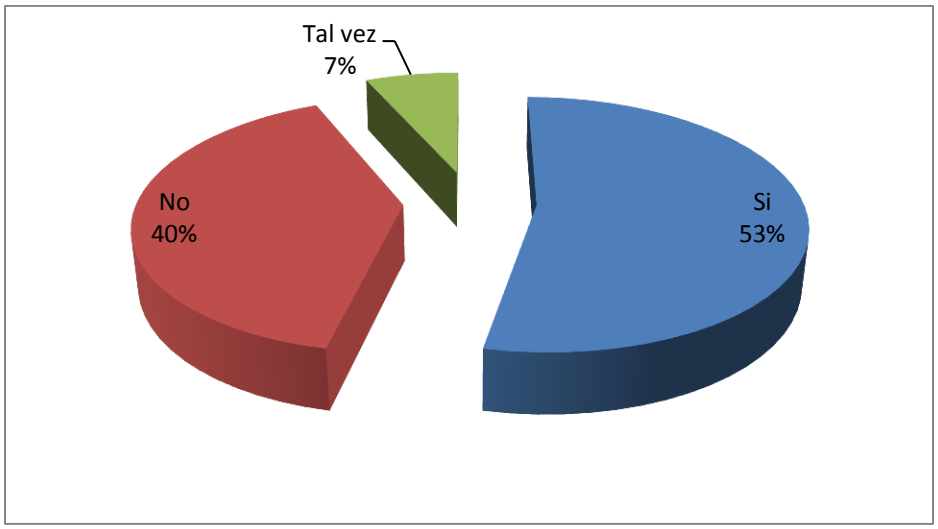


Gráfico: 4.25 Padres de familia donde expresan si conocen sus hij@s lo que es pornografía (Elaborado por: Investigador)

El 53,33% de los padres de familia dice que su hij@ si sabe lo que es pornografía, el 40% de los padres de familia dice que su hij@ no sabe lo que es pornografía, y el 6,67% dicen que su hij@ tal vez sabe lo que es pornografía.

Pregunta: ¿Sabe si su hijo@ ha visto pornografía en Internet?

Si	No	Tal vez
1	14	0

Tabla 4.32 Tabulación encuesta dirigida a los padres de familia, sobre si conoce si su hij@ ha visto pornografía en Internet (Elaborado por: Investigador).

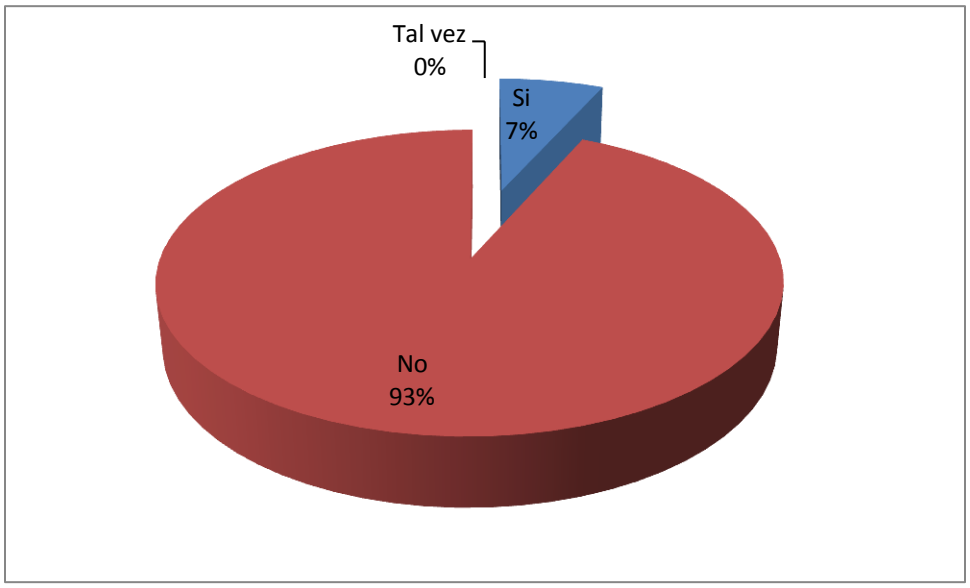


Gráfico: 4.26 Padres de familia donde expresan si conoce si su hij@ ha visto pornografía en Internet (Elaborado por: Investigador)

El 6,67% de los padres de familia dice que su hijo@ si ha visto pornografía, el 93,33% de padres de familia dice que no sabe si su hij@ no ha visto pornografía, y el 0% asume que su hij@ tal vez ha visto pornografía.

Pregunta: ¿Sabe si su hij@ ha tenido acceso a pornografía en Internet en forma accidental?

Si	No	Tal vez
2	12	1

Tabla 4.33: Tabulación encuesta dirigida a los padres de familia, donde expresan si saben si sus hij@s han tenido acceso a pornografía en Internet en forma accidental (Elaborado por: Investigador).

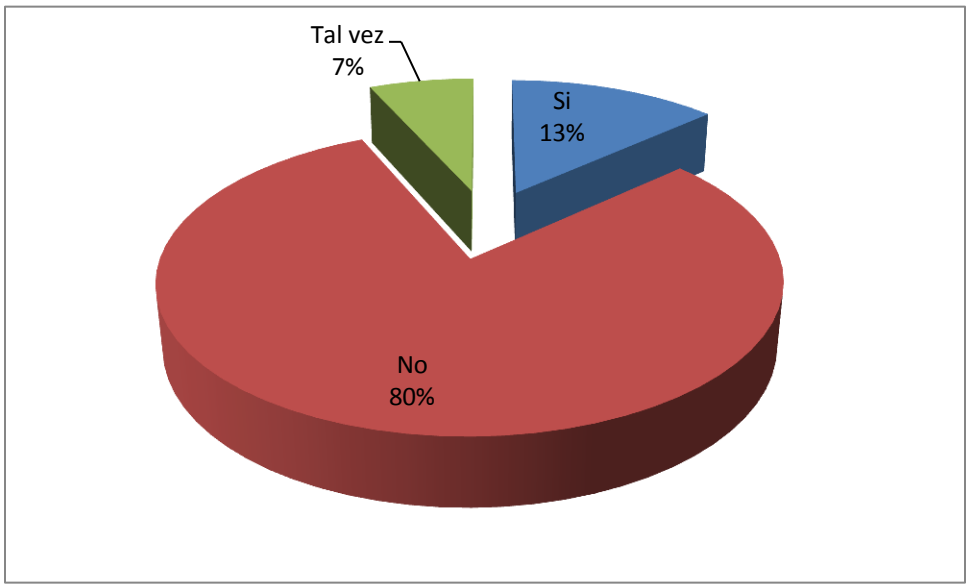


Gráfico: 4.27 Padres de familia donde expresan si saben si sus hij@s han tenido acceso a pornografía en Internet en forma accidental (Elaborado por: investigador)

El 13,33% de los padres de familia dice que su hijo(a) ha tenido acceso a pornografía en Internet en forma accidental, el 80% de los padres de familia dice que su hijo(a) no ha tenido acceso a Internet en forma accidental y el 6,67% dice que su hijo(a) tal vez pudo haber tenido acceso a Internet en forma accidental.

Pregunta: ¿Sabe si su hij@ ha tenido propuestas inadecuadas en Internet por desconocidos?

Si	No	Tal vez
2	13	0

Tabla 4.34: Tabulación encuesta dirigida a los padres de familia, donde expresan si saben si sus hij@s han tenido propuestas inadecuadas en Internet por desconocidos (Elaborado por: Investigador).

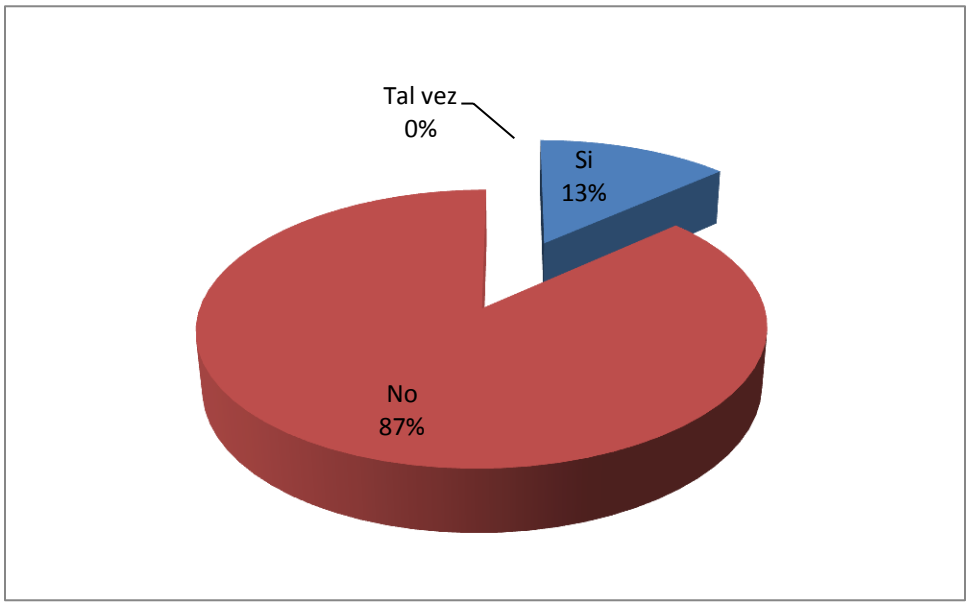


Gráfico: 4.28 Padres de familia donde expresan si saben si sus hij@s han tenido propuestas inadecuadas en Internet por desconocidos (Elaborado por: Investigador).

El 13,33% de los padres de familia dice que su hij@ ha tenido propuestas inadecuadas en Internet por desconocidos, el 86,67% dice que su hijo@ no ha tenido propuestas inadecuadas en Internet por desconocidos.

Pregunta: ¿Sabe lo que es cyberbulling?

Si	No	Tal vez
11	4	0

Tabla 4.35: Tabulación encuesta dirigida a los padres de familia, sobre si conocen el significado de cyberbulling (Elaborado por: Investigador).

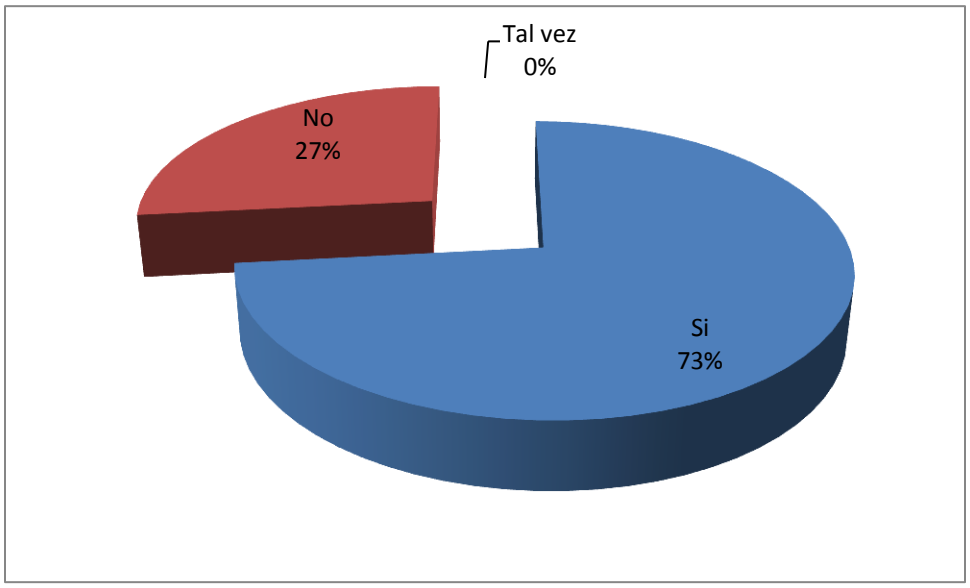


Gráfico: 4.29 Padres de familia que expresan si conocen el significado de cyberbulling (Elaborado por: Investigador)

El 73,33 % de padres de familia dice que sus hij@s si saben lo que es cyberbulling, el 26,67% de los padres de familia dicen que sus hij@s no saben lo que es cyberbulling y el 0% dice que tal vez saben lo que es cyberbulling.

Pregunta: ¿Sabe si su hij@ ha sido víctima de algún engaño en Internet?

Si	No	Tal vez
1	14	0

Tabla 4.36: Tabulación encuesta dirigida a los padres de familia, donde expresan si sus hij@s han sido víctimas de algún engaño en Internet (Elaborado por: Investigador).

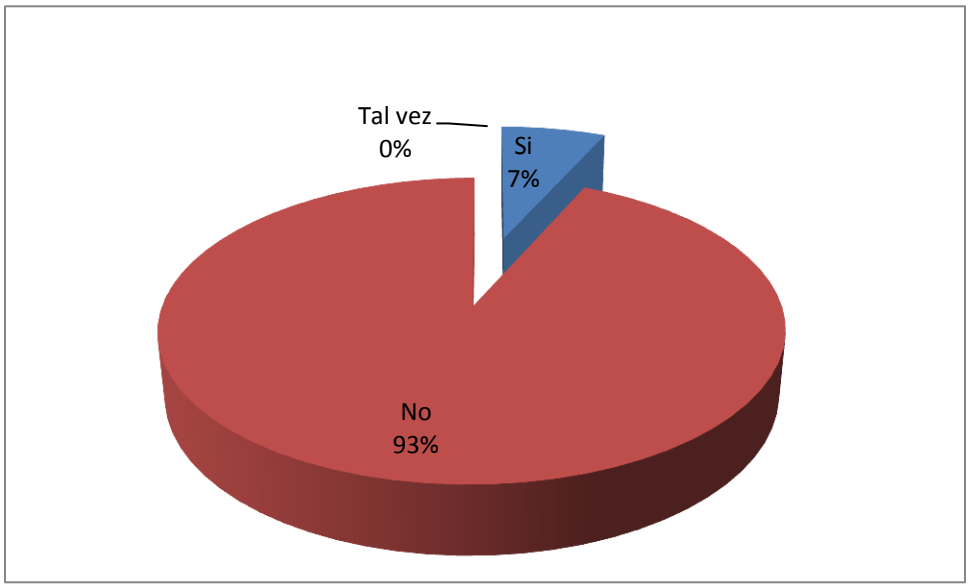


Gráfico: 4.30 Tabulación de Encuestas dirigida a los padres de familia sobre los peligros de Internet (Elaborado por: Investigador)

El 6,67% de los padres de familia dice que su hij@ si ha sido víctima de algún engaño en Internet, el 93,33% dice que su hij@ no ha sido víctima de algún engaño en Internet y el 0% dice que tal vez su hij@ ha sido víctima de algún engaño en Internet.

Pregunta: Cuando a su hij@ le aparece en Internet alguna imagen inadecuada a su edad que cree que haría su hij@?

Le avisa a sus padres	Le cuenta a un adulto	Comenta con un profesor	Comenta con algún compañero	Se queda callado	Ninguna de las anteriores	No contesta
8	2	1	1	0	1	1

Tabla 4.37: Tabulación de Encuesta dirigida a los padres de familia sobre lo que hacen los niños, niñas y adolescentes cuando ven una imagen inadecuada en Internet (Elaborado por: Investigador)

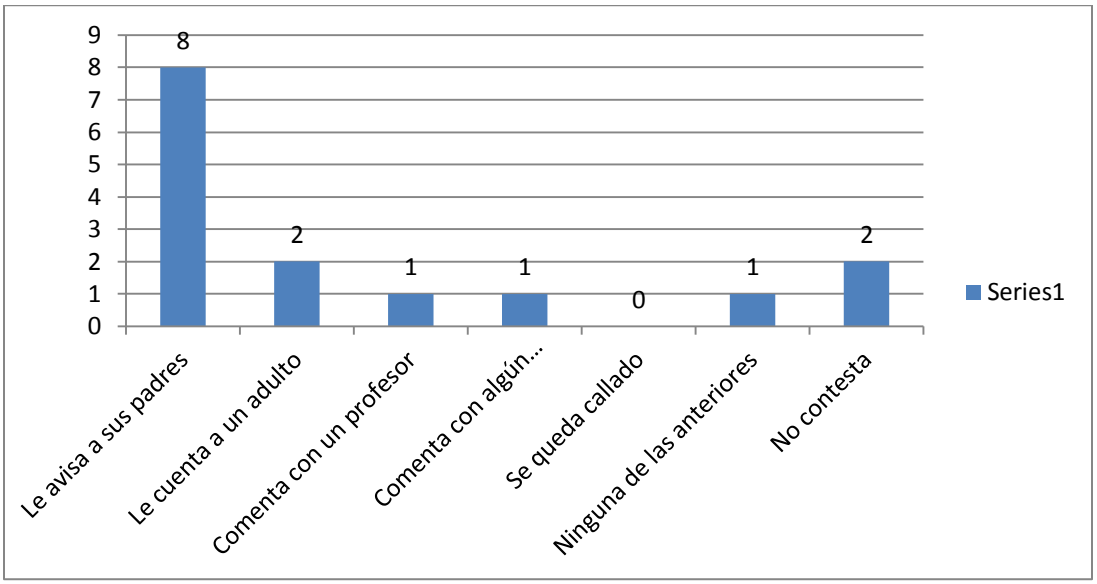


Gráfico: 4.31 Tabulación de encuesta dirigida a los padres de familia sobre lo que hacen sus hij@s cuando ven una imagen inadecuada en Internet (Elaborado por: Investigador)

El 53.33 % de los padres de familia consideran que sus hijos les avisarían si les apareciera alguna imagen inadecuada a su edad; el 13,33% consideran que sus hijos le contarían a un adulto, el 6,67% consideran que comentarían con un profesor, el 6,67% considera que comentaría con algún compañero, el 0% considera que su hijo(a) se quedaría callado, el 6,67% considera que su hijo no haría ninguna de las anteriores, y el 13,33% no contesta la pregunta.

4.1.10 Comparación de resultados de la encuesta dirigida a los estudiantes y padres de familia sobre los peligros de Internet

4.1.10.1 Indicador: Internet

Pregunta H: Hijo(a) P(Padres de familia)	Padres de familia	Hijos(as)	Comparación de respuestas padres de familia versus respuestas de sus hijos(as) sobre peligros del Internet
1. H: ¿Sabe lo que es pornografía? P: ¿Sabe si su hijo(a) conoce lo que es porno-grafía?	El 53,33% de los padres de familia dice que su hijo (a) si sabe lo que es pornografía, el 40% dice que su hijo(a) no sabe y El 6,67% dice que su hijo(a) tal vez sabe lo que es pornografía.	El 50% de los estudiantes si sabe lo que es pornografía, y el 50% dice que no sabe qué es pornografía	El 3,33 % de padres de familia piensa que su hijo si sabe lo que es pornografía, mientras que el 50% concuerda en sus respuestas. El 40% de padres de familia duda y el 6,67% dice que tal vez, lo que implicaría que el 46,67% de padres de familia no sabe o duda si su hijo(a) sabe lo que es pornografía versus el 50% de sus hijos(as) que confirman no saber qué es pornografía.

Tabla 4.34: Comparación de resultados de la encuesta dirigida a los estudiantes y padres de familia sobre los peligros de Internet (Elaborado por: Investigador) (cont.)

Tabla 4.34: Comparación de resultados de la encuesta dirigida a los estudiantes y padres de familia sobre los peligros de Internet (cont.)

Pregunta **H: Hijo(a)** **P(Padres de familia)**	**Padres de familia**	**Hijos(as)**	**Comparación de respuestas padres de familia versus respuestas de sus hijos(as) sobre peligros del Internet**
2. H: ¿Ha visto pornografía en Internet? P: ¿Sabe si su hijo(a) ha visto pornografía en Internet?	El 6,67% de los padres de familia dice que su hijo(a) si ha visto pornografía en Internet El 93,33% de padres de familia dice que no sabe si su hijo(a) no ha visto pornografía en Internet. El 0% asume que su hijo(a) tal vez ha visto pornografía en Internet.	El 34,62 % de los estudiantes si han visto pornografía en Internet El 61,54% no ha visto pornografía en Internet. 3,85 % tal vez ha visto pornografía en Internet.	El 27,95 % de los padres de familia desconocen que sus hijos(as) han visto pornografía en Internet; el 6,67% concuerda que si ha visto pornografía en Internet. El 61,54% de los padres de familia concuerdan que sus hijos(as) no han visto pornografía en Internet, mientras que el 31,79% de los Padres de Familia no sabe si su hijo(a) ha visto pornografía en Internet. El 3,85% de los estudiantes manifiestan que tal vez ha visto pornografía en Internet versus el 0% de sus Padres.

Tabla 4.34: Comparación de resultados de la encuesta dirigida a los estudiantes y padres de familia sobre los peligros de Internet (Elaborado por: Investigador) (cont.)

Tabla 4.34: Comparación de resultados de la encuesta dirigida a los estudiantes y padres de familia sobre los peligros de Internet (cont.)

Pregunta **H: Hijo(a)** **P(Padres de familia)**	**Padres de familia**	**Hijos(as)**	**Comparación de respuestas padres de familia versus respuestas de sus hijos(as) sobre peligros del Internet**
3. H: ¿Ha tenido acceso a pornografía en forma accidental? P: ¿Sabe si su hijo ha tenido acceso a pornografía en forma accidental?	El 13,33% de los padres de familia dice que si sabe que su hijo(a) ha tenido acceso a pornografía en Internet en forma accidental. El 80% de los padres de familia dice que no sabe si su hijo(a) ha tenido acceso a pornografía en Internet en forma accidental, y el 6,67% dice que su hijo(a) tal vez	El 38,46 % de los estudiantes ha tenido acceso a pornografía en forma accidental, El 61,54% de los estudiantes no ha tenido acceso a internet en forma accidental.	El 13,33% de los padres de familia concuerdan con las respuestas de sus hijos(as) en que si han tenido acceso en Internet en forma accidental, el 25,13 % de los padres de familia desconoce que sus hijos si han tenido acceso a pornografía en forma accidental. El 61,54% de los estudiantes confirma que no ha tenido acceso a Internet en forma accidental y el 80% padres de familia no sabe si sus hijos(as) han tenido acceso a Internet en forma accidental. Concuerda con las respuestas de sus hijos(as) en que no han tenido acceso a Internet en forma accidental; mientras que el 18,54% de los padres

Tabla 4.34: Comparación de resultados de la encuesta dirigida a los estudiantes y padres de familia sobre los peligros de Internet (Elaborado por: Investigador) (cont.)

Tabla 4.34: Comparación de resultados de la encuesta dirigida a los estudiantes y padres de familia sobre los peligros de Internet (cont.)

Pregunta **H: Hijo(a)** **P(Padres de familia)**	**Padres de familia**	**Hijos(as)**	**Comparación de respuestas padres de Familia versus respuestas de sus hijos(as) sobre peligros del Internet**
…	pudo haber tenido acceso a Internet en forma accidental.	…	de familia cree que sus hijos(as) no han tenido acceso a Internet en forma accidental.
4. H: ¿Ha tenido propuestas inadecuadas en Internet por desconocidos? P: ¿Sabe si su hijo ha tenido propues-tas inadecuadas en Internet por	El 13,33% de los padres de familia dice que su hijo(a) ha tenido propuestas inadecuadas en Internet por desconocidos. El 86,67% dice que sabe si su hijo(a) ha tenido propuestas inadecuadas en Internet por	El 30,77% de estudiantes si ha tenido propuestas inadecuadas en Internet. El 61,54 % de los estudiantes no ha tenido propuestas inadecuadas en	El 13,33% está enterado(a) que sus hijos(as) han tenido propuestas inadecuadas por desconocidos en Internet, mientras que el 17,44% de padres de familia desconoce que sus hijos(as) han tenido propuestas inadecuadas por desconocidos en Internet. El 61,54% de los Estudiantes confirma no ha tenido propuestas inadecuadas en Internet, mientras que el 86,67% de sus Padres no sabe si sus hijos(as) han tenido propuestas inadecuadas

Tabla 4.34: Comparación de resultados de la encuesta dirigida a los estudiantes y padres de familia sobre los peligros de Internet (Elaborado por: Investigador) (cont.)

Tabla 4.34: Comparación de resultados de la encuesta dirigida a los estudiantes y padres de familia sobre los peligros de Internet (Cont.)

Pregunta **H: Hijo(a)** **P(Padres de familia)**	**Padres de familia**	**Hijos(as)**	**Comparación de respuestas padres de Familia versus respuestas de sus hijos(as) sobre peligros del Internet**
…desconocidos?	…desconocidos.	…Internet El 7,69% de los estudiantes tal vez ha tenido propuestas inadecuadas en Internet.	…en Internet. El 7,69% de los estudiantes se reserva el derecho contestando que tal vez ha tenido propuestas inadecuadas en Internet, mientras que Los padres de familia nadie optó por esta opción.
5. H: ¿Sabe lo que es cyberbulling? P: ¿Sabe lo que es cyberbulling?	El 73,33 % de padres de Familia si saben lo que es cyberbulling, el 26,67% de los padres de familia no saben lo que es cyberbulling.	El 100% de los estudiantes no saben lo que es cyberbulling.	El 73,33% de los padres de familia si saben los que es cyberbulling, más sin embargo sus hijos(as) el 100% no sabe lo que es cyberbulling. El 26,67% de los padres de familia no saben lo que es cyberbulling.

Tabla 4.34: Comparación de resultados de la encuesta dirigida a los estudiantes y padres de familia sobre los peligros de Internet (Elaborado por: Investigador) (cont.)

Tabla 4.34: Comparación de resultados de la encuesta dirigida a los estudiantes y padres de familia sobre los peligros de Internet (cont.)

Pregunta **H: Hijo(a)** **P(Padres de familia)**	**Padres de familia**	**Hijos(as)**	**Comparación de respuestas padres de Familia versus respuestas de sus hijos(as) sobre peligros del Internet**
6. H: ¿Ha sido víctima de algún engaño en Internet? P: ¿Sabe si su hijo(a) ha sido víctima de algún engaño en Internet?	El 6,67% de los padres de familia dice que su hijo(a) si ha sido víctima de algún engaño en Internet. El 93,33% dice que no sabe si su hijo(a) ha sido víctima de algún engaño en Internet, el 0% dice que tal vez su hijo(a) ha sido víctima de algún engaño en Internet.	El 15,38% de los estudiantes si ha sido víctima de algún engaño en Internet. El 84,62% no ha sido víctima de algún engaño en Internet.	El 6,67% de los padres de familia coincide con las respuestas de sus hijos(as), mientras que un 8,71% de ellos desconoce que su hijo(a) ha sido víctima de algún engaño en Internet. El 84,62% de los estudiantes confirma que no ha sido víctima de algún engaño en Internet; más sin embargo el 93,33% de padres de familia confirma no saber si su hijo(a) ha sido víctima de algún engaño en Internet, sin siquiera dar lugar a un tal vez.

Tabla 4.34: Comparación de resultados de la encuesta dirigida a los estudiantes y padres de familia sobre los peligros de Internet (Elaborado por: Investigador) (cont.)

Tabla 4.34: Comparación de resultados de la encuesta dirigida a los estudiantes y padres de familia sobre los peligros de Internet (cont.)

Pregunta **H: Hijo(a)** **P(Padres de familia)**	**Padres de familia**	**Hijos(as)**	**Comparación de respuestas padres de Familia versus respuestas de sus hijos(as) sobre peligros del Internet**
7. H: Cuando a usted le aparece en Internet alguna imagen inadecuada a su edad ¿qué hace? P: Cuando a su hijo(a) le aparece en Internet alguna imagen inadecuada a su edad que cree que haría su hijo(a)?	El 53.33 % de los padres de familia consideran que sus hijos les avisarían si les apareciera alguna imagen inadecuada a su edad.	El 15,38% les avisa a sus padres cuando le aparece en Internet alguna imagen inadecuada a su edad.	El 37,95 % de los padres de familia no se imaginan que sus hijos se no les avisarían a sus Padres si encontraran una imagen inadecuada en internet y el 15,38 % acertarían en la respuesta que sus hijos(as) actuarían ante tal situación.
	El 13,33% consideran que sus hijos le contarían a un adulto.	El 19,23 % le cuenta a un adulto.	El 5.9% de los padres de familia menos que sus hijos piensan que le contarían a un adulto si ve una imagen inadecuada en Internet.
	El 6,67% consideran que comentarían con un profesor.	El 3,85% le comenta a un profesor.	El 2,82% de los padres de familia más que los estudiantes piensan que no lo comentarían con un Profesor si sus hijos ven una imagen inadecuada en Internet.

Tabla 4.34: Comparación de resultados de la encuesta dirigida a los estudiantes y padres de familia sobre los peligros de Internet (Elaborado por: Investigador) (cont.)

Tabla 4.34: Comparación de resultados de la encuesta dirigida a los estudiantes y padres de familia sobre los peligros de Internet (cont.)

Pregunta **H: Hijo(a)** **P(Padres de familia)**	**Padres de familia**	**Hijos(as)**	**Comparación de respuestas padres de Familia versus respuestas de sus hijos(as) sobre peligros del Internet**
…	El 6,67% considera que comentaría con algún compañero.	15,38 % comenta con algún compañero.	El 8.71% menos de los Padres de Familia piensan que le dirían a un compañero si ven una imagen inadecuada en Internet.
	El 0% considera que su hijo(a) se quedaría callado(a).	y el 46,15% se queda callado(a).	El 46,15% de los padres de familia desconocen que su hijo(a) se quedaría callado(a)
	El 6,67% considera que su hijo(a) no haría ninguna de las anteriores.	0%	El 6,67% de los padres de familia considera que su hijo(a) no haría ninguna de las cosas anteriores si ve una imagen inadecuada en internet.
	El 13,33% no contesta la pregunta.	0%	El 13,33% de los padres de familia se abstiene de contestar la pregunta a diferencia de sus hijos(as).

Tabla 4.38: Comparación de resultados de la encuesta sobre los peligros de Internet, padres de familia e hijos(as)
(Elaborador por: Investigador)

4.2 Interpretación de datos

De las entrevistas, visitas técnicas realizadas, se puede determinar que el CELP no dispone de políticas sobre seguridad informática, existe la inversión en tecnología más sin embargo no hay nadie quien asuma la responsabilidad del área y de seguimiento de forma permanente; también se evidencia una falta de compromiso con los Propietarios ya que la oficina en la que se encuentran actualmente los equipos de comunicaciones pasa cerrada y no tienen acceso a encender el servidor y el switch que da conectividad al área administrativa, únicamente puede entrar su Propietario.

El Profesor de Tic hace lo que puede, ya que no dispone de material adicional, o manejo de claves para poder realizar actualizaciones de antivirus, sistemas operativos, software de navegación, entre otros; tampoco existe la comunicación adecuada entre el Profesor de TICs y el Encargado de Tecnología que visita el establecimiento únicamente cuando hay un daño físico y en horas no laborables y la única persona encargada de llamarlo es el Propietario, por ende el software utilitario instalado originalmente se mantiene sin cambio alguno a pesar de que el Profesor manifiesta requerir nuevas versiones para dictar sus clases.

En Talento Humano existe buena organización, y fue nuevo para la persona encargada los temas que deben ser incluidos sobre seguridad informática en este ámbito.

En cuanto al Desarrollo del Sistema de Gestión que ya debió implantarse a inicios del año lectivo 2013 -2014, el problema es el mismo no hay quien haga seguimiento y la persona desarrolladora es externa, no dispone de tiempo para ir entre semana a capacitar al Personal para el manejo del mismo, no ha entregado manuales al Propietario, intentó hacer pruebas pero el sistema no trabajó como es debido por los problemas de la red que tiene la Institución ya que la Secretaria de la Institución se demoraba en ingresar al sistema más de 15 minutos; y dado que pasa a formar parte de los activos de la Institución y se relaciona con la formación de los estudiantes ya que tiene un módulo en el que los docentes ingresan

tareas y los padres de familia pueden ver lo que deben hacer sus hijos por medio de Internet, los docentes aún no saben cómo utilizarlo y cuando intentan los problemas de red y de hardware no les permite ingresar al mismo.

Sobre los Peligros del Internet en la comparación de las encuestas padres e hijos resulta lo siguiente:

- El 46,67% de padres de familia no sabe o duda si su hijo(a) sabe lo que es pornografía.
- 31,79% de los padres de familia no sabe si su hijo(a) ha visto pornografía en Internet.
- El 25,13 % de los padres de familia desconoce que sus hijos si han tenido acceso a pornografía en forma accidental.
- El 80% padres de familia no sabe si sus hijos(as) han tenido acceso a pornografía en Internet en forma accidental.
- El 13,33% está enterado(a) que sus hijos(as) han tenido propuestas inadecuadas por desconocidos en Internet, mientras que el 17,44% de padres de familia desconoce que sus hijos(as) han tenido propuestas inadecuadas por desconocidos en Internet.
- El 61,54% de los estudiantes confirma no ha tenido propuestas inadecuadas en Internet, mientras que el 86,67% de sus padres no sabe si sus hijos(as) han tenido propuestas inadecuadas en Internet.
- El 7,69% de los estudiantes se reserva el derecho contestando que tal vez ha tenido propuestas inadecuadas en Internet, mientras que los padres de familia nadie optó por esta opción.
- El 73,33% de los padres de familia si saben los que es cyberbulling, más sin embargo sus hijos(as) el 100% no sabe lo que es cyberbulling.
- El 26,67% de los padres de familia no saben lo que es cyberbulling.

- El 6,67% de los padres de familia coincide con las respuestas de sus hijos(as), mientras que un 8,71% de ellos desconoce que su hijo(a) ha sido víctima de algún engaño en Internet.
- El 84,62% de los estudiantes confirma que no ha sido víctima de algún engaño en Internet; más sin embargo el 93,33% de padres de familia confirma no saber si su hijo(a) ha sido víctima de algún engaño en Internet, sin siquiera dar lugar a un tal vez.
- El 46,15% de los padres de familia desconoce que su hijo(a) se quedaría callado(a) si ve una imagen inadecuada en Internet; el 37,95% de los estudiantes no les avisarían a sus padres si encuentran una imagen inadecuada en Internet; lo que suma 84,10% de padres de familia desconoce que sus hijos(as) se quedarían callados(as) o no les avisarían a ellos; porcentaje extremadamente alto que evidencia que los riesgos de los niños, niñas y adolescentes al navegar en Internet sin seguridades son altos.

4.3 Verificación de Hipótesis

Las hipótesis planteadas son:

En primer lugar se plantea una hipótesis (Hi) y una hipótesis (H0).

Hi: La seguridad informática incide en la formación de niños, niñas y adolescentes de Educación Inicial y Básica del Centro Educativo La Pradera.

H0: La seguridad informática no incide en la formación de niños, niñas y adolescentes de Educación Inicial y Básica del Centro Educativo La Pradera.

Nivel de significación

El nivel de significación escogido para la prueba fue del 5% o 0,05.

Elección de la Prueba Básica

Para la verificación de la hipótesis se escogió la prueba de Ji-cuadrado cuya fórmula es la siguiente:

$$X^2 = \frac{\sum(O - E)^2}{E}$$

Ecuación 1: Estadístico de prueba Ji-cuadrado

Donde

$$X^2 = Ji - cuadrado$$

$$\sum \quad = Sumatoria$$

$O = Datos\ observados$ ($Medición\ del$ log producto del monitoreo)

$= Datos\ esperados$ (Medición del log producto del monitoreo)

Para la comprobación de la hipótesis se procede a relacionar dos tablas una referente a seguridad con los estudiantes y la otra referente a formación con los docentes.

Se utilizó el log generado en el squid que está en el servidor proxy, y para gestionar la información generada se utilizó un software de gestión Sawmill ver 8.0 de evaluación (ver anexo 22) de logs de squid y luego fueron tabulados en excel para hacer el conteo de las páginas web.

La siguiente tabla se genera del log tomado con los estudiantes de 5to, 6to, 7mo. (Ver log en Anexo 14).

	Páginas autorizadas	**Otras páginas**	**Páginas pornográficas**
Estudiantes	7	9	3
Docentes	8	7	4
Total	15	16	7

Tabla 4.39: Tabla de contingencia - generada del log de estudiantes de 5to, 6to, 7mo y docentes navegando en Internet el 5 de noviembre del 2013 (Elaborado por: Investigador)

Zona de Aceptación o Rechazo

$$\boldsymbol{Grados\ de\ Libertad\ (gl) = (f-1)(c-1)}$$

Ecuación 2: Grados de libertad:

Donde (gl) = Grado de libertad

c = Columnas de la Tabla

f = Filas de la Tabla

Reemplazando:

$$(gl) = (fila - 1)(columna - 1)$$
$$(gl) = (f - 1)(c - 1)$$
$$(gl) = (2 - 1)(3 - 1)$$
$$(gl) = (1)(2)$$
$$(gl) = 2$$

El valor tabulado del Ji-cuadrado X^2 con dos grados de libertad y un nivel de significación del 5% o 0,5 es de 5,99, como se puede observar en la gráfica 4.32 generada con el programa PQRS.

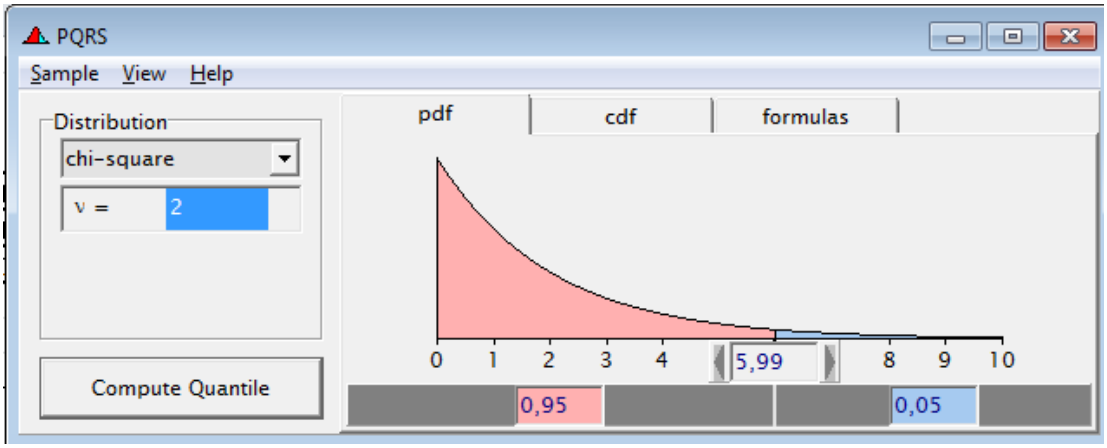


Gráfico: 4.32 Gráfica de Distribución Ji-cuadrado (Elaborado por: Investigador)

Luego se procede a realizar la tabla de frecuencias observadas versus frecuencias esperadas para el cálculo X^2.

	Categoría	O	E	(O-E)	(O-E)2	(O-E)2 /E
Estudiantes	Acceso a páginas autorizadas	7.00	5.00	2.00	4.00	0.80
	Otras páginas	9.00	5.33	3.67	13.44	2.52
	Páginas pornográficas	3.00	2.33	0.67	0.44	0.19
Docentes	Acceso a páginas autorizadas	8.00	5.00	3.00	9.00	1.80
	Otras páginas	7.00	5.33	1.67	2.78	0.52
	Páginas pornográficas	4.00	3.50	0.50	0.25	0.07
						5.90

Tabla 4.40: Tabla de contingencia - generada del log de estudiantes y docentes navegando en Internet el 5 de noviembre del 2013 (Elaborado por: Investigador)

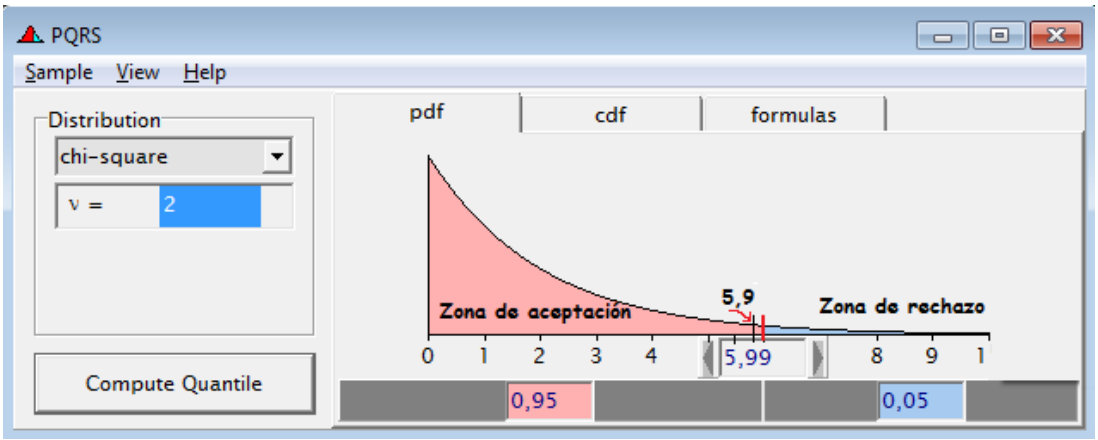


Gráfico: 4.33 Gráfica de demostración de Hipótesis usando la Distribución Ji-cuadrado (Elaborado por: Investigador)

Cae en la zona de aceptación por lo que se acepta la hipótesis alternativa "Hi: La seguridad informática relacionada a la utilización de Internet como herramienta de apoyo incide en la formación de niños, niñas y adolescentes de Educación Inicial y Básica del Centro Educativo La Pradera" y se rechaza la hipótesis nula H0.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

- Se determinó mediante la prueba JI-cuadrado que la seguridad informática incide en la utilización del Internet como herramienta de apoyo en la formación de niños, niñas y adolescentes de Educación Inicial y Básica del CELP.
- De las entrevistas realizadas al Encargado de Tecnología, Propietario y Jefe de Recursos Humanos se concluye que el CELP no tiene definidas políticas, procedimientos o estándares de seguridad informática para la utilización de internet como herramienta de apoyo, ni en el resto de áreas.
- La formación que permite la utilización de Internet como herramienta de apoyo en la formación de niños, niñas y adolescentes del CELP es insegura ya que el Internet se encuentra sin restricción alguna.
- Existe un desconocimiento del uso de herramientas guiadas para búsquedas en internet como webquest, cazas de tesoro como lo evidencian los resultados de la encuesta ya que el 100% de Docentes desconoce de las herramientas mencionadas.
- El 57% de Docentes no dirige las investigaciones a sitios seguros, el 29% si, dirige sus Investigaciones a sitios seguros y el 14% no sabe lo que son sitios seguros, lo que significa que los estudiantes están expuestos a las amenazas de Internet.
- Con respecto a la encuesta realizada a los Estudiantes y padres de familia sobre los peligros de Internet se concluye que la mayoría de los padres de familia desconoce

sobre lo que hace su hijo(a) ante los peligros de Internet, y tampoco existe una buena comunicación, lo que significa que es alto el riesgo que corren los niños, niñas y adolescentes ante una amenaza como lo evidencia el análisis de resultados realizado.

5.2 Recomendaciones

- Hacer un Plan de Seguridad Informática en el que se involucre a todo el talento humano en pro de mejorar la seguridad en la formación de los niños, niñas y adolescentes del CELP.
- Definir políticas, procedimientos de seguridad informática para la utilización de internet como herramienta de apoyo aplicando el estándar ISO 27001.
- Colocar seguridades a nivel de red para que la utilización del Internet como herramienta de apoyo en la formación de niños, niñas y adolescentes del CELP mejore la seguridad.
- Capacitar continuamente al personal docente en herramientas Tics que puedan ser aplicadas en el aula como herramientas de apoyo en clases.
- Hacer talleres de socialización a los padres de familia sobre los peligros de Internet y la Seguridad informática.

CAPÍTULO VI

LA PROPUESTA

Nombre de la propuesta

Plan de Gestión de Seguridad Informática para el Centro Educativo La Pradera

6.1 Datos Informativos

El Centro Educativo La Pradera CELP es una institución educativa de carácter privado, se dedica a formar niños, niñas y adolescentes, tiene educación Inicial y educación Básica.

Sus valores son educar con paz, amor, respeto, tolerancia, compromiso, puntualidad, disciplina y lealtad.

Sus principios son: trabajo en equipo, servicios, cultura de buen trato, comunicación, equidad.

Se encuentra ubicado en Cantón Rumiñahui, Parroquia Sangolquí, en la Av. General Enríquez 2900 y Río Chinchipe. Sus propietarios Arq. Luis Atapuma, Sra. Zoila Díaz de Atapuma.

6.2 Antecedentes de la Propuesta

El CELP tiene como visión “Complacer las expectativas educacionales que van acorde al nuevo milenio”, lo que involucra ir a la par con el avance tecnológico y para ello dotar de continuas capacitaciones a los DOCENTES involucrando a los padres de familia en el sistema integral de sus hijos a través de la dispersión recreativa, cultural, deportiva y tecnológica que crea espacios de comunicación familiar.

La misión es merecer la excelencia total: brindando al mundo estudiantes analíticos, reflexivos, críticos, creativos y preparados para enfrentar los nuevos retos tecnológicos.

El objetivo de forjar estudiantes con magnífico nivel académico sólidos en valores para que puedan competir con eficiencia y eficacia en la incansable lucha contra las duras tareas del diario vivir.

Ya los docentes del mundo empiezan a evidenciar los peligros que conllevan el uso del Internet y a la vez los beneficios gigantes que existen, es así que La Junta de Castilla y León – Consejo de Cataluña en su portal Guía para el Profesorado y Centros Escolares textualmente dice: “Es recomendable que se cuente con un plan de educación en seguridad informática. De esta forma, al tiempo que se aprende a utilizar las Nuevas Tecnologías, se toma conciencia de los beneficios y los potenciales peligros que existen en la red” (Junta de Castilla y León - Consejería de Educación, 2013, pág. 1).

En Ecuador el Ministerio de Telecomunicaciones (Mintel), en base a encuestas a 4,8 millones de alumnos de escuelas y colegios, públicos y privados, determinó que la conexión doméstica a Internet es la forma más habitual de navegación en menores de edad. De ese total, millones de niños tienen de 6 a 9 años y el 63% dijo tener conexión online en la casa y el colegio. El porcentaje baja al 57% en chicos de 10 a 18 años, que alcanzan 1,8 millones, según el estudio del Mintel "La generación interactiva en Ecuador" (Diario Hoy, 2012)

La psicóloga y terapeuta alternativa de niños y adolescentes Daysi Guzmán señala en un artículo del diario Hoy de Ecuador "las cifras evidencian las crecientes amenazas que representa el ciberespacio para los menores de edad. "En el Ecuador hay poca educación sobre el uso de Internet en padres e hijos y las instituciones educativas no tratan con énfasis el tema. La concienciación en seguridad informática debería iniciar a los cinco años" (Diario Hoy, 2012)

6.3 Justificación

Esta propuesta se justifica porque cuenta con el apoyo de los propietarios del CELP además de tener infraestructura propia de la cual pueden disponer de acuerdo a las necesidades de la Institución.

Cada año sus dueños invierten 25% de sus ingresos para mejoras en tecnología.

6.4 Objetivos

6.4.1 Objetivo General

Diseñar un Plan de gestión de la seguridad Informática usando la norma ISO 27001:2005 para fortalecer la seguridad de los estudiantes en materia de TI.

6.4.2 Objetivos Específicos

Rediseñar la Red del CELP para que esté acorde a las necesidades de la institución y permita un crecimiento tecnológico sostenido.

Definir políticas, normas, procedimientos, controles para la gestión de seguridad de la información, tales como hardware, software, red, estudiantes.

Delinear un plan de capacitación al personal docente sobre las nuevas técnicas de uso de Internet como herramienta de apoyo en el aula.

Proponer un taller de capacitación a los padres de familia sobre los riesgos, amenazas de Internet y herramientas para ayudar a prevenir los mismos.

Evaluar la propuesta del Plan de Seguridad Informática.

6.5 Análisis de Factibilidad

La Institución cuenta con un área de mejor iluminación de 10,5 m x 6,5 m que equivale a 68,25 metros cuadrados en donde se puede hacer el Centro de Comunicaciones y el Laboratorio de Tics.

6.5.1 Técnica

Plan de seguridad informática es técnicamente factible ya que la Institución cuenta con una persona encargada de tecnología y un profesor de Tics de planta que puede asumir el rol de encargado de la seguridad de la informática.

Se cuenta con los Planos del CELP para realizar el rediseño de la red, la experiencia del investigador en el área, un servidor de aplicaciones, y existe el presupuesto para la adquisición de los equipos de comunicaciones, materiales que se requieren.

Es técnicamente factible ya que el CELP cuenta con equipos como: computadores, proyector para realizar la capacitación de la aplicación de Tics, como herramienta de apoyo el Internet para el personal docente al igual que para el Taller de riesgos, amenazas de Internet y herramientas para ayudar a prevenir los mismos dirigido a Padres de Familia

6.5.2 Operativa

La operatividad del Plan de seguridad informática es factible ya que cuenta con la colaboración del Profesor de Tics, al igual que del encargado de tecnología para que se mantenga y se implemente el SGSI.

El rediseño de la red es operativo ya que ayudará a resolver los problemas internos generados en el CELP como el acceso adecuado al sistema de gestión de información, control de acceso seguro a la red e internet, estará instalado de tal forma que tengan todo el tiempo los servicios de comunicaciones internos, lo que garantizará que si deja de funcionar uno de los switch, la red no se va a caer y que siga funcionando la misma

La operación del Plan de capacitación al personal docente de la aplicación de Tics como herramienta de apoyo en Internet para el personal docente al igual que para el Taller de riesgos, amenazas de Internet y herramientas para ayudar a prevenir los mismos dirigido a Padres de Familia es factible ya que cuenta con la predisposición de las autoridades, personal docente y padres de familia para adquirir estos conocimientos, lo que garantizará que los niños, niñas y adolescentes del CELP se encuentren protegidos de los peligros del Internet.

6.5.3 Económica

El costo de la implementación y mantenimiento del Plan de seguridad de la Información es factible ya que se requiere incurrir en gastos de materiales de oficina, papel, tinta, archivadores y tiempo de quien asuma el rol de coordinador de la seguridad de informática.

El costo de la implementación de la red podrá ser incluida el 50% este año y el otro 50% con el presupuesto de tecnología del Plan de mejoras del año 2014-2015.

Es económicamente factible ya que el costo de la capacitación al personal docente de la aplicación de Tics como herramienta de apoyo en Internet para el personal docente será pagado por los mismos docentes; el Taller de riesgos, amenazas de Internet y herramientas para ayudar a prevenir los mismos dirigido a Padres de Familia será subsidiado por el fondo de mantenimiento de tecnología que aportan los Padres de Familia en la matrícula.

6.5.4 Equidad Organizacional

El Centro Educativo La Pradera se encuentra debidamente organizado ya que se basa en lo estipulado en la LOEI.

6.5.5 Equidad de Género

Esta propuesta está dirigida a hombres y mujeres que se encuentren en cargos de Dirección, en Jefaturas, Profesores (as) de Tics, de las instituciones educativas que quieran impulsar, o aplicar la seguridad Informática sobre una infraestructura de red adecuada.

6.5.6 Ambiental

Esta propuesta al ser integral porque así lo requiere la ISO 27001:2005, y cada elemento de la seguridad de la información se relaciona entre si tomando en cuenta a las personas, repercute directamente ya que obliga a tener un ambiente seguro con normas establecidas, con conciencia de los docentes, estudiantes y padres de familia y por ende un ambiente positivo de trabajo y de confianza.

6.5.7 Legal

El Centro Educativo La Pradera está legalmente constituido, tiene la aprobación del Ministerio de Educación para funcionar desde educación inicial hasta educación básica (1ro a 7mo), se encuentra en un período de legalización de 8vo y 9no y está regido bajo la Ley orgánica institucional del Ecuador.

6.6 Fundamentación

La presente propuesta toma en cuenta los lineamientos dados en la norma ISO 27001:2005 en la parte referente a Planear o establecer un Plan de Seguridad de la Información del Sistema de Gestión de, cuya base es el análisis de riesgos que presenta en la ISO 27005.

La norma ISO 27001:2005 "fue preparada por el Comité Técnico ISO /IEC JTC1, Tecnologías de la Información, Subcomité 27, Técnicas de seguridad TI." (ISO/ICE, ITC, 2005, pág. 4), en donde manifiesta que está basado en el modelo PDCA cuyas siglas en español constituyen Planear – Hacer – Chequear – Actuar.

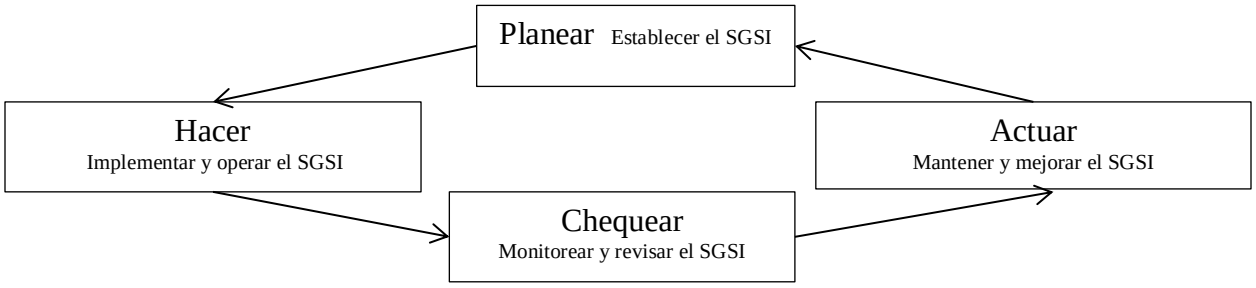


Gráfico: 6.1 Modelo PDCA aplicado a los procesos SGSI (Fuente:ISO/ICE:27001, ITC, 2005)

El "Planear" significa establecer políticas, objetivos, procesos, procedimientos para el Plan de Seguridad Informática que sea relevante para manejar el riesgo y mejorar la seguridad y que se puedan entregar resultados en el área educativa en concordancia con los objetivos generales de la Institución. (ISO/ICE, ITC, 2005, pág. 8).

Dentro de la norma ISO 27001:2005 se establece terminología importante que vale la pena citarla:

"Activo, es cualquier cosa que tenga valor para la organización" (ISO/IEC, 13335-1:2004) (ISO/ICE, ITC, 2005, pág. 9), en este concepto la norma ISO toma en cuenta a las personas como activo de valor para la organización.

"Seguridad de la información es la preservación de la confidencialidad, integridad y disponibilidad de la información, además, también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no repudio y confiabilidad" (ISO/IEC, 17799:2005)" (ISO/ICE, ITC, 2005, pág. 10), a continuación se definen los conceptos de confidencialidad, integridad y disponibilidad.

"Disponibilidad es la propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada (ISO/IEC, 13335-1:2004)" (ISO/ICE, ITC, 2005, pág. 9), la disponibilidad es un factor muy importante a la hora de realizar la valuación de activos, ya que de nada sirve tener activos y cuando se necesiten no poder utilizarlos a causa de una mala gestión.

"Integridad es la propiedad de salvaguardar la exactitud e integridad de los activos. (ISO/IEC, 13335-1:2004)" (ISO/ICE, ITC, 2005, pág. 10), para las instituciones educativas constituye la integridad del proceso de negocio de negocio principal que es la formación de niños, niñas y adolescentes, laboratorio de Tics, equipos del área administrativa, equipos de comunicaciones entre otros.

"Confidencialidad es la propiedad que esta información esté disponible y no sea divulgada a personas, entidades o procesos no – autorizados. (ISO/IEC, 13335-1:2004)" (ISO/ICE, ITC, 2005, pág. 9), la confidencialidad es otra propiedad en la que la información (hardware, software, redes, medios, interfaces, información en sí) que se encuentra disponible no sea divulgada a terceros no autorizados.

"Evento de seguridad de la información es una ocurrencia identificada del estado de un sistema, servicio o red indicando una posible violación de la política de seguridad de la información o falla en las salvaguardas, o una situación previamente desconocida que puede ser relevante para la seguridad (ISO/IEC, TR 18044:2004)" (ISO/ICE, ITC, 2005, pág. 10).

"Incidente de seguridad de la información es un solo o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una significativa probabilidad de comprometer las operaciones comerciales y amenazan la seguridad de la información (ISO/IEC, TR 18044:2004)" (ISO/ICE, ITC, 2005). Para el caso del área educativa de carácter privado una falta de seguridad en el control de acceso a Internet si compromete las operaciones comerciales que en este caso constituirían pago de pensiones o de acuerdo a la

gravedad retiro de los niños, niñas de la institución educativa, disminuye la credibilidad de la Institución.

“Sistema de gestión de seguridad de la información SGSI, esa parte del sistema gerencial general (estructura organizacional, políticas, actividades de planeación, responsabilidades, prácticas, procedimientos, procesos, y recursos) basada en un enfoque de riesgo comercial, para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.” (ISO/ICE, ITC, 2005, pág. 10).

Para mayor detalle ver la terminología en el glosario de términos.

Para el análisis de riesgo la norma ISO 27005:2008 recomienda seguir el siguiente proceso:

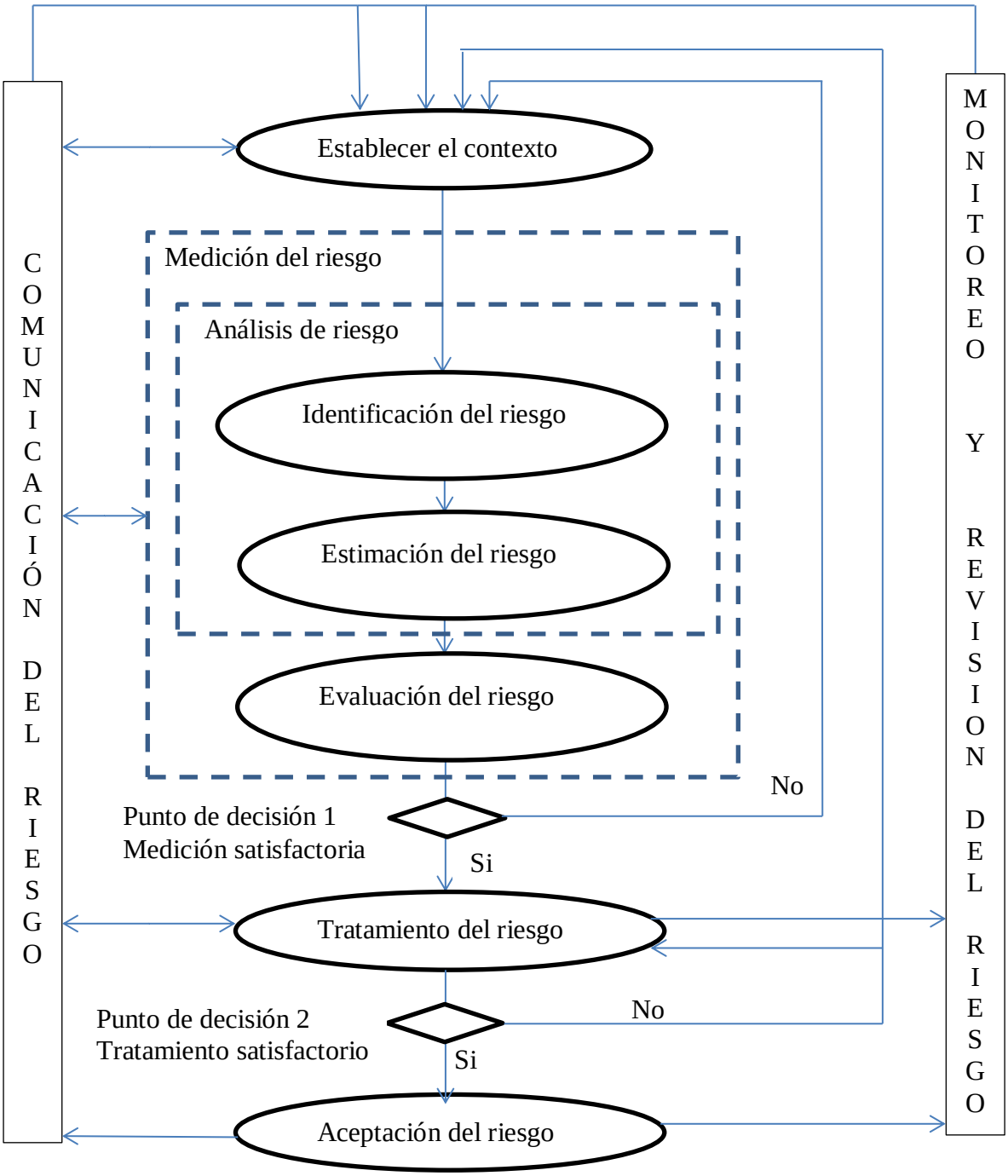


Gráfico: 6.2 Proceso de administración de riesgos (Fuente: IEC/ITS 27005,2008,pág 5)

6.7 Metodología

La metodología utilizada para realizar el Plan de Seguridad Informática sigue los pasos propuestos en la norma ISO 27001:2005.

a) Definir el alcance y los límites del SGSI en términos de las características del negocio, la organización, su ubicación, activos, tecnología e incluyendo los detalles de y la justificación de cualquier exclusión del alcance.
b) Definir una política SGSI en términos de las características del negocio, la organización, su ubicación, activos y tecnología.
c) Definir el enfoque de valuación de riesgo de la organización.
d) Identificar riesgos.
e) Analizar y evaluar el riesgo.
f) Identificar y evaluar las opciones para el tratamiento de los riesgos.
g) Seleccionar objetivos de control y controles para el tratamiento de los riesgos.
h) Obtener aprobación de la gerencia para los riesgos residuales propuestos.
i) Obtener la autorización de la gerencia para implementar y operar el SGSI.
j) Preparar un enunciado de aplicabilidad.

La metodología a aplicar para el re diseño de la red es la siguiente:

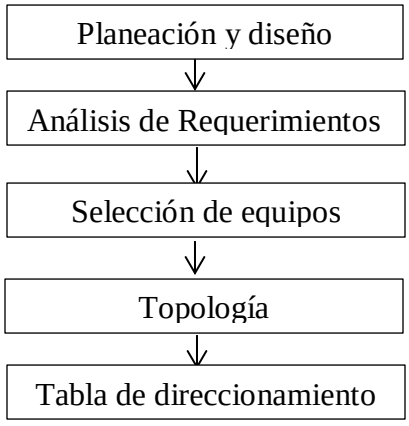


Gráfico: 6.3 Metodología para Diseño de Red (Elaborado por: Investigador)

6.8 Modelo Operativo

6.8.1 Diagnóstico de la Situación actual

6.8.1.1 Esquema de Red actual

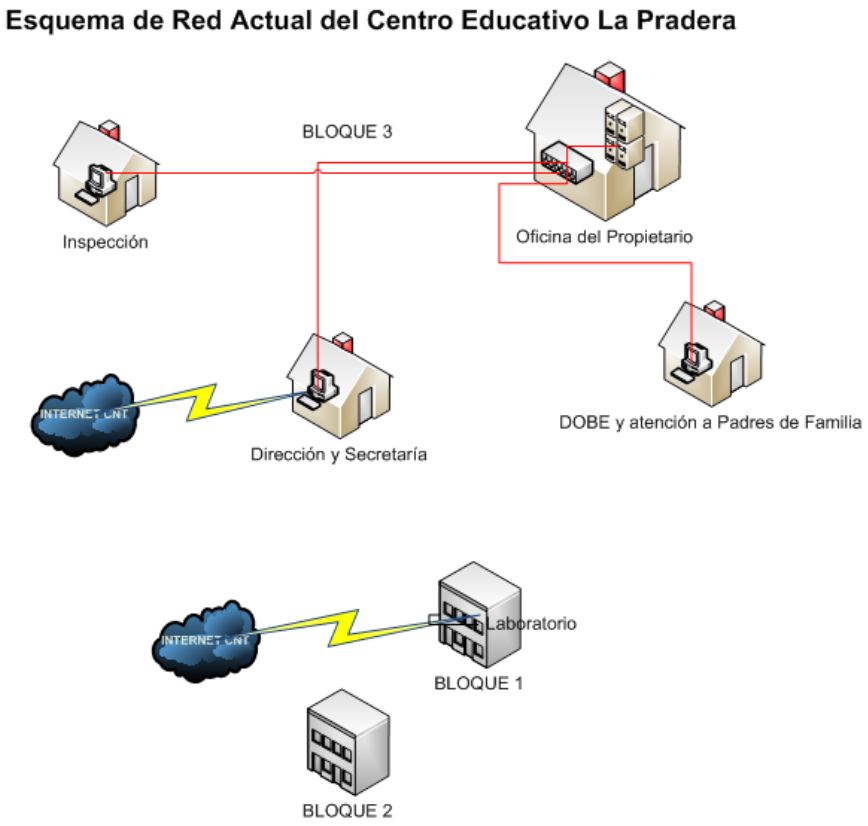


Gráfico: 6.4 Esquema de red actual del CELP (Elaborado por: Investigador)

Aplicando los lineamientos descritos en la Norma ISO 27005, una vez estimado el riesgo, hay que tomar decisiones realizando el tratamiento de riesgo en donde se tiene las siguientes opciones:

- Reducción de riesgo
- Retención del riesgo
- Evitación del riesgo

- Transferencia del riesgo

Luego de analizar el tratamiento de riesgo a seguir se propone hacer el rediseño de la red, establecer políticas y controles necesarios para cada etapa, hacer un plan de capacitación para docentes sobre seguridades y herramientas guiadas, y un taller para padres de familia sobre ventajas y riesgos del uso de Internet así como también soluciones tecnológicas.

Para ello se propone el trabajo en 5 fases como se describen a continuación:

Fase 1: Establecer el Plan de Seguridad Informática

Fase 2: Rediseño de la red

2.1 Análisis de requerimientos

2.2 Selección de equipos

2.3 Selección de materiales

2.4 Topología física

2.5 Tabla de direccionamiento

Fase 3: Realizar un plan de capacitación para docentes sobre seguridades y herramientas guiadas.

Fase 4: Realizar un taller para padres de familia sobre ventajas y riesgos del uso de Internet así como también soluciones tecnológicas

Fase 5: Presentación y evaluación de la propuesta.

6.8.2 Plan de seguridad Informática

6.8.2.1 **Definición de seguridad de la información**

"Seguridad de la información es la preservación de la confidencialidad, integridad y disponibilidad de la información, además, también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no repudio y confiabilidad (ISO/IEC 13335-1:2004)" (IEC/ITC ISO 27001, 2005, pág. 10).

6.8.2.2 **Objetivos**

- Disminuir el riesgo para fortalecer la seguridad integral del Centro Educativo La Pradera.
- Comprometer a todo el elemento Humano: propietarios, personal docente, personal administrativo, estudiantes, padres de familia con el proceso de seguridad, agilizando la aplicación de los controles con dinamismo y armonía.
- Ganar calidad y prestigio institucional con la prestación del servicio de seguridad.

6.8.2.3 **Alcance y Límites**

El presente Plan involucra las siguientes áreas y elemento humano como son:

- Hardware
- Software utilitario del Laboratorio y área administrativa
- Comunicaciones
- Red del Centro Educativo La Pradera
- Estudiantes
- Propietarios
- Docentes
- Administrativos
- Padres de familia

6.8.2.4 **Importancia**

Es importante tener un Plan de Seguridad Informática o Plan de Seguridad de la Información ya que de nada sirve tener inversión en activos tecnológicos como son hardware, software, redes, medios, comunicaciones, sistemas, bases de datos entre otros si no se da el seguimiento adecuado y responsable sobre los riesgos que esto involucra como es el área educativa donde se están formando niños, niñas y adolescentes en lo que respecta a formación que es el proceso de negocio más importante de una entidad educativa, ya que la calidad académica va de la mano con la seguridad y por ende con las utilidades generadas por brindar un servicio de excelencia.

6.8.2.5 **Enunciado de intención de los Propietarios**

Enunciado de intención de los Propietarios			
Fecha de emisión:	**Fecha de modificación**	**Fecha de aprobación**	**Indicador. D-PRO-01**
Elaborado por:		**Revisado y aprobado por:**	

I. INTRODUCCIÓN

El presente documento presenta el enunciado de intención de los propietarios con el CELP

II. ENUNCIADO DE INTENCIÓN DE LOS PROPIETARIOS

Con la finalidad de forjar y formar estudiantes con magnífico nivel académico sólidos en valores que puedan competir con eficiencia y eficacia en la incansable lucha contra las duras tareas del diario vivir de una manera segura se plantea el presente documento con las políticas necesarias para disminuir el riesgo que conlleva el uso de tecnología sin las seguridades adecuadas.

Cabe mencionar la gran necesidad de elevar el nivel académico y competitivo con la finalidad de captar más estudiantes que quieran estudiar en una Institución con tecnología de punta de forma segura, lo que dará tranquilidad a los padres de familia de que sus hijos se encuentran protegidos de las amenazas del Internet.

Se aplicarán y se dará seguimiento a las políticas, normas, procedimientos establecidos en el presente documento para garantizar el cumplimiento del mismo de acuerdo al alcance establecido.

Firman

Arq. Luis Atapuma — PROPIETARIO

Lic. Zoila Días de Atapuma — PROPIETARIA

Documento 1: Enunciado de intención de los Propietarios (Elaborado por: Investigador)

6.8.2.6 **Marco Referencial**

El marco referencial permite establecer los objetivos de control y los controles incluyendo la estructura de la evaluación de riesgo y la gestión de riesgo.

6.8.2.6.1 Identificación del riesgo

6.8.2.6.2 Propósito de la administración del riesgo

Describir los requerimientos de seguridad informática para el control de acceso a Internet del CELP.

Establecer un plan de seguridad informática para el Centro Educativo La Pradera.

Alcance y límites

- Objetivo del Centro Educativo La Pradera

  Forjar y formar estudiantes con magnífico nivel académico sólidos en valores para que puedan competir con eficiencia y eficacia en la incansable lucha contra las duras tareas del diario vivir.

- Proceso de negocio

  El proceso de negocio del área educativa se apoya en los siguientes documentos:

  Plan Educativo Institucional es un proceso de reflexión y acción estratégica de la comunidad educativa, es un documento público de planificación estratégica institucional en el que constan acciones estratégicas a mediano y largo plazo, dirigidas a asegurar la calidad de los aprendizajes y una vinculación propositiva en el entorno escolar (Art. 88 del Reglamento de la LOEI)

El Plan de mejora es un instrumento para identificar y organizar las respuestas de cambio ante las debilidades encontradas en la autoevaluación institucional.

Código de convivencia que es un documento con un conjunto de directrices generales elaborado con la intención de que todo proceso formativo gire alrededor de los principios de autonomía, autogestión y participación, donde todos aporten en la construcción de un contexto propicio a la convivencia pacífica, basada en el respeto mutuo y en los deseos permanentes de superación. El Plan de convivencia es parte fundamental del PEI (Plan Educativo Institucional), se basa en los artículos 89,90 del reglamento a la Ley Orgánica de Educación Intercultural (LOEI)

- **Estructura**

Organigrama

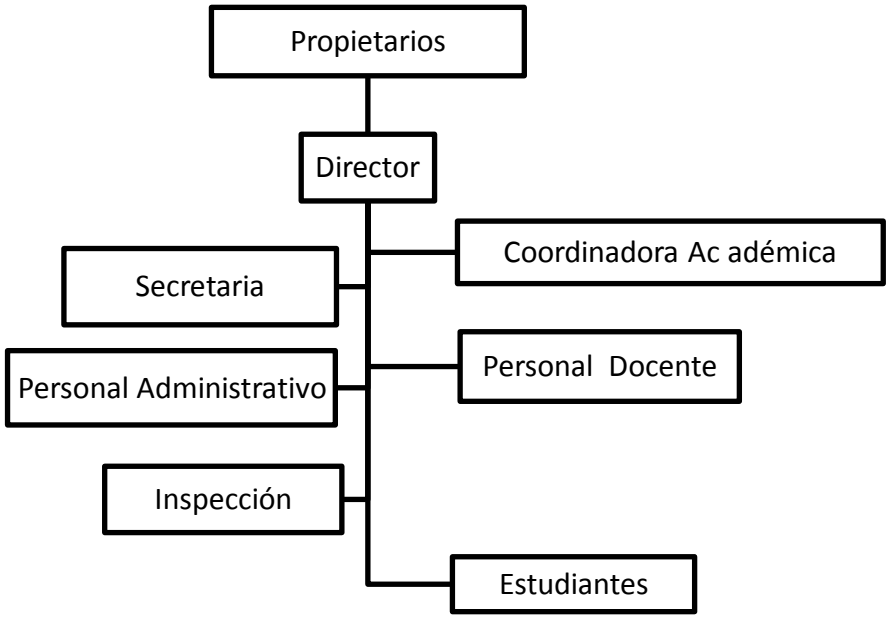


Gráfico: 6.5 Organigrama del Centro Educativo La Pradera (Elaborado por: Investigador)

- Los requisitos legales

  Marco Legal Educativo está la Ley orgánica de Educación Intercultural y reglamento general.
- No tienen definidas políticas de seguridad de la información.
- La gestión de riesgos de la organización.

  Disponen del Plan Institucional de Gestión de Riesgos cuyo objetivo es implementar estrategias de prevención emergencia y recuperación de eventos adversos, dentro y fuera del contexto en el que se desarrolla la comunidad educativa a través de la preparación y socialización de un plan de gestión de riesgos.
- Información de los activos, está a cargo de Lic. Viviana Sanguano
- Localización de la organización y sus características geográficas

  Provincia: Pichincha Cantón Rumiñahui

  Parroquia: Sangolquí – Valle de los Chillos Barrio: San Jorge

  Ingreso 1: Av. General Enríquez 2900 y Río Chinchipe

  Ingreso 2: Río Yaupi 1-76, Barrio San Jorge

Restricciones que afectan a la organización

Que se deriva de un Clima político económico	Evaluación del Ministerio de Educación a los Centros educativos. Disminución de estudiantes matriculados durante el año lectivo 2012 – 2013
Restricciones del personal docente	No tienen acceso a Internet cuando lo necesitan
Restricción relacionada a métodos	Acuerdo para legalizar 8vo, 9no, 10mo

Tabla 6.1: Restricciones que afectan a la Institución (Fuente: IEC/ITC ISO 27005, 2008, Págs 26,27) (Elaborado por: Investigador)

Lista de referencias regulatorias legislativas aplicables en la organización

Las leyes están regidas por la LOEI, Ley Orgánica de Educación Intercultural, que en el capítulo IV, sección III, Art. 53 en Funciones del Consejo Ejecutivo en el numeral 5, dice "Diseñar e implementar estrategias para la protección integral de los estudiantes;" (LOEI, 2011, pág. 18) y en el capítulo VIII, art. 342 numeral 4 menciona "realizar el seguimiento en el ámbito educativo del cumplimiento de las medidas de protección dictadas por las autoridades competentes en la protección de los estudiantes".

Restricciones que afectan al enfoque

Técnicas	Archivos Sistema de Gestión de Información Software Hardware Redes y comunicaciones
Ambientales	Riesgos naturales Situación geográfica Clima
Estructurales	En el organigrama no consta un encargado de TI
Métodos	Profesor Tics Encargado de Tecnología
Organizacionales	Mantenimiento Gestión administrativa

Tabla 6.2: Restricciones que afectan al enfoque (Fuente: IEC/ITC ISO 27005, 2008, Págs 26,27) (Elaborado por: Investigador)

Expectativas de las partes interesadas

Propietario: Comprender cómo se beneficia la Institución con la puesta en práctica de la misma.

Docentes: Tener acceso continuo a Internet para usar como herramienta de apoyo

Estudiantes: Usar Internet en el Laboratorio cuando necesiten

6.8.2.6.3 Inventario de Activos

Gráfico: 6.6 Fotografía Jefe RRHH con información de Inventario de Activos (Elaborado por: Investigador)

"Activo, es cualquier cosa que tenga valor para la organización" (ISO/IEC, 13335-1:2004) (ISO/ICE, ITC, 2005, pág. 9), para el trabajo de esta investigación utilizando la norma ISO 27001, son tomadas en cuenta las personas como activos.

El inventario de activos lo proporciona Lic. Viviana Sanguano quien es la encargada de los Activos de la Institución.

Se procede a generar un código de Identificación para el Activo con la siguiente estructura: las dos primeras letras son el departamento al que pertenecen, los 3 últimos dígitos son la numeración asignada por la responsable de entregar los activos y designar sus propietarios, por motivos de seguridad no se detallará las características de cada activo en detalle.

Inventario de activos

Identificación	Tipo	Activo	Descripción	Propietario	Ubicación física
DA001	Datos	Base de Datos	Motor MySQL contiene información del sistema de gestión de información de la Institución	Arq. Luis Atapuma	OF005
DA002		Registro de Matrículas	Archivo en Excel de matrículas de estudiantes	Lic. Cecilia Rodríguez	OF001
DA003		Información de Calificaciones	Archivo Excel de calificaciones entregadas por el personal docente	Lic. Cecilia Rodríguez	OF001
DA004		Cobro de Pensiones	Archivo en Excel del cobro de pensiones de la institución	Lic. Cecilia Rodríguez	OF001
DA005		Información Histórica de los Egresados	Archivos en Excel de cada año con información histórica de notas, pensiones, entre otros	Lic. Cecilia Rodríguez	OF001

Tabla 6.3: Inventario de Activos del CELP (Elaborado por: Investigador) (Fuente: IEC/ITC 27005, 2008, pág. 10) (cont.)

Tabla 6.3: Inventario de Activos del CELP (Elaborado por: Investigador) (cont.)

Identificación	Tipo	Activo	Descripción	Propietario	Ubicación física
DA006		Documentación recibida vía email del Ministerio de Educación Documentación enviada al Ministerio de Educación	Archivos pdf	Lic. Cecilia Rodríguez	OF001
SO001	Aplicaciones	Página Web	Página web publicada en un hosting fuera de la institución, que presenta reportes de notas de los estudiantes	Encargado de Tecnología	Hosting EEUU
SO002	Aplicaciones	Sistema de Gestión de la Información del CELP Página Web	Sistema integrado que involucra, matrículas, representantes, pensiones, calificaciones, tareas entre otros	Arq. Luis Atapuma	OF005

Tabla 6.3: Inventario de Activos del CELP (Fuente: IEC/ITC 27005, 2008, pág. 10) (Elaborado por: Investigador) (cont.)

Tabla 6.3: Inventario de Activos del CELP (Elaborado por: Investigador) (cont.)

Identificación	Tipo	Activo	Descripción	Propietario	Ubicación física
SE001	Servicios	Página web	Visualizar Notas, Deberes, Separación de cupos, Eventos	Encargado de Tecnología	EEUU
	Tecnología	Computador	Computador que distribuye el internet en la red administrativa	Lic. Cecilia Rodríguez	OF001
		Impresora	Destinada para el uso exclusivo de documentación de la institución	Lic. Cecilia Rodríguez	OF001
		Computador	Computador para uso del Personal Administrativo e Inspección	Lic. Viviana Sanguano	OF002
		Teléfono	Teléfono para hacer llamadas a los padres de familia en caso de emergencias	Lic. Viviana Sanguano	OF002
		Impresora	Impresora destinada para el uso de documentos de inspección y del personal docente	Lic. Viviana Sanguano	OF002

Tabla 6.3: Inventario de Activos del CELP (Fuente: (IEC/ITC 27005, 2008, pág. 10)) (Elaborado por: Investigador) (cont.)

Tabla 6.3: Inventario de Activos del CELP (Elaborado por: Investigador) (cont.)

Identificación	Tipo	Activo	Descripción	Propietario	Ubicación física
 DO001	… Tecnología	Computador	Computador	Lic. Paola Ushiña	OF003
 DI-001		1 Servidor	Servidor donde se encuentra instalado el Sistema de Gestión de Información y la Base de Datos	Arq. Luis Atapuma	OF005
 DI-002		1 Switch	Equipo de comunicaciones que conecta el área Administrativa en Red	Arq. Luis Atapuma	OF005
 LA0018		1 Router	Router 3com que permite distribuir el Internet en la Wireless	Lic. David De La Cruz	OF007
 LA001 a la  LA015		Equipo Informático del Laboratorio	8 computadores, CPUs Intel CD 7 computadores CPUs Intel PIV 15 Monitores Samsung Flat Panel de 17 pulgadas	Lic. David De La Cruz	OF007

Tabla 6.3: Inventario de Activos del CELP (Fuente: IEC/ITC 27005, 2008, pág. 10) (Elaborado por: Investigador) (cont.)

Tabla 6.3: Inventario de Activos del CELP (Elaborado por: Investigador) (cont.)

Identificación	Tipo	Activo	Descripción	Propietario	Ubicación física
CA001	… Tecnología	Cableado Estructurado	Se encuentra en el interior de las oficinas indicadas que pertenecen al área administrativa y pasa por los exteriores de las mismas	Área Administrativa	OF001- OF002- OF003- OF004- OF005- OF006
	Instalaciones	Oficina de Secretaría	Se encuentra a mano derecha de la puerta de ingreso a la institución	Lic. Cecilia Rodríguez	OF001
		Inspección	Se encuentra a mano izquierda de la puerta de ingreso a la institución	Lic. Viviana Sanguano	OF002
		DOBE	Se encuentra al lado derecho de secretaría	DOBE	OF003
		Dirección	Se encuentra en el segundo piso de secretaría	Arq. Luis Atapuma	OF004

Tabla 6.3: Inventario de Activos del CELP (Fuente: IEC/ITC 27005, 2008, pág. 10) (Elaborado por: Investigador) (cont.)

Tabla 6.3: Inventario de Activos del CELP (Elaborado por: Investigador) (cont.)

Identificación	Tipo	Activo	Descripción	Propietario	Ubicación física
	Instalaciones	Propietarios	Se encuentra frente a la oficina del DOBE	Sra. Zoila de Atapuma Arq. Luis Atapuma	OF005
	… Instalaciones	Recepción de Padres de familia	Se encuentra en la planta baja del DOBE	Conserjería	OF006
		Laboratorio de TICs	Se encuentra en el segundo piso del bloque 2	Lic. David De La Cruz	OF007
	Equipamiento Auxiliar	Router CNT	Router que permite conectarse con la CNT para proporcionar servicio de Internet al Laboratorio	Lic. Cecilia Rodríguez	OF001
		Router CNT	Router que permite conectarse con la CNT para proporcionar servicio de Internet al Laboratorio	Lic. David De La Cruz	OF007

Tabla 6.3: Inventario de Activos del CELP (Fuente: IEC/ITC 27005, 2008, pág. 10) (Elaborado por: Investigador) (cont.)

Tabla 6.3: Inventario de Activos del CELP (Elaborado por: Investigador) (cont.)

Identificación	Tipo	Activo	Descripción	Propietario	Ubicación física
	Equipamiento auxiliar	Línea telefónica	Línea telefónica CNT 022333550	Lic. Cecilia Rodríguez	OF001
		Línea telefónica	Línea telefónica CNT 022334995	Lic. David De La Cruz	OF007
		Línea telefónica	Línea telefónica privada CNT	Dueños	OF005
PRO001 PRO002 PRO003 … PRO008 PA001	Personal	Personal de Planta del Centro Educativo Personal Subcontratado Padres de familia	Personal Administrativo integrado por: Inspectora, Secretaria, Coordinadora Académica, Conserje, Director Personal subcontratado integrado por: Responsable de tecnología, Desarrollador. Padres de familia	Dueños de la Institución	OF001 a OF005 AU001 AU002 … AU008

Tabla 6.3: Tabla de Inventario de Activos del CELP (Fuente: IEC/ITC 27005, 2008, pág. 10) (Elaborado por: Investigador)

Se procede a identificar los activos que se relacionan con la presente investigación quedando el siguiente listado:

6.8.2.6.4 Identificación de los activos

De la identificación de activos sale la siguiente lista con procesos de negocio.

Activos Principales

Procesos de negocio

Cobro de pensiones

Formación de niños, niñas y adolescentes

Información

Matrículas

Cuentas por cobrar

Históricos

Autoevaluación Institucional

Proyecto Plan Institucional

Plan de Mejora

Financiera

Activos de apoyo

Hardware

Equipo de procesamiento de datos

Equipos fijos

Procesamiento de periféricos

Medios para datos

Medios electrónicos

Otros medios

Software

Sistema de Gestión de Información

Página Web

Microsoft Office

Sistema Operativo

Windows 7

Windows XP

Servicio de mantenimiento o administración del software

Paquetes de software

My sql

Matemáticas, Inglés

Redes

Soporte y medios

CNT

Ethernet

Wireless

Dispositivos de comunicaciones

Router

Switch

Interfaz de comunicaciones

Tarjetas inalámbricas

Tarjetas ethernet

Personal

Toma de decisiones

Propietario - Director

Coordinadora Académica

Inspectora

Docentes

Planta de tutores y profesores especiales

Desarrolladores

Encargado de desarrollo del sistema de gestión de información

Sitio

Oficinas administrativas

Laboratorio

Localización

Servicios esenciales

Energía eléctrica

Comunicación

Teléfono

Internet

Organización

Estructura de la organización

6.8.2.6.5 Valuación de los activos

El siguiente paso luego de la identificación de activos es establecer la escala de valuación para cada activo, hay activos que pueden valuarse por su valor monetario pero otros como la información, o las personas no tienen una representación económica, por lo que se elige la siguiente escala:

Escala de valuación: Bajo, Medio, Alto

Activos Principales

Tipo	Activo	Criterio de valuación	Valuación	Valuación del activo
Proceso de negocio	Formación de niños, niñas y adolescentes	Poner en peligro la seguridad de los estudiantes	Alto	Alto
		Interrupción del servicio	Medio	
		Daño de la reputación	Alto	

Tabla 6.4: Valuación de Activo: Procesos de Negocio (Fuente: IEC/ITC 27005, 2008, págs. 35-37) (Elaborado por: Investigador)

Valuación de Activos de apoyo

Tipo	Activo	Criterio Consecuencias	Valuación	Valuación del activo
Hardware	Equipos fijos Computadores del Laboratorio TICs	Pérdida de la reputación	Alto	Alto
		Pérdida del activo	Alto	
		Baja la calidad educativa	Alto	
	Servidor de control de acceso a Internet	Interrupción del servicio de Internet	Alto	Alto
Software	Sistema Operativo	Pérdida de confianza de los padres de familia	Alto	Alto
		Pérdida de credibilidad	Alto	
		Pérdida en la reputación	Alto	
		Violación de leyes	Alto	
	Servicio de mantenimiento o administración del software	Costo interno adicional	Bajo	Medio
		Costo financiero para emergencias o reparaciones	Bajo	
		Daños materiales	Medio	
	Paquetes de software Matemáticas, Inglés Microsoft Office	Interrupción en el servicio	Medio	Medio

Tabla 6.5 Valuación de activos de apoyo (Elaborado por: Investigador) (cont.)

Tabla 6.5 Valuación de activos de apoyo (cont.)

Tipo	Activo	Criterio Consecuencias	Valuación	Valuación del activo
	Antivirus	Poner en peligro la seguridad de los estudiantes	Alto	Alto
		Deterioro del rendimiento del equipo	Bajo	
	Navegadores para Internet	No pueden verse correctamente las páginas web	Alto	Alto
Redes	Soporte y medios Red pública	Poner en peligro la seguridad de los estudiantes Los docentes no pueden preparar sus clases utilizando material de Internet	Alto	Alto
	Ethernet Wireless 802.11 a/b/c/n/g	Interrupción del servicio de red	Medio	Alto
		Pérdida de competitividad	Alto	
	Dispositivos de comunicaciones Router Switch	Formación académica de los estudiantes	Alto	Alto
		Preparación de material e investigación de los docentes	Alto	
		Pérdida económica	Bajo	

Tabla 6.5 Valuación de activos de apoyo (Elaborado por: Investigador) (cont.)

Tabla 6.5 Valuación de activos de apoyo (cont.)

Tipo	Activo	Criterio Consecuencias	Valuación	Valuación del activo
	Interfaz de comunicaciones Tarjetas de red inalámbricas Tarjetas de red Ethernet	Costo interno adicional al navegar en Internet	Bajo	Alto
		Deteriora el rendimiento del laboratorio	Medio	
		Interrupción del servicio de red	Medio	
		Los estudiantes no pueden hacer uso del Internet para aprender	Alto	
Personal	Toma de decisiones Propietario – Director	Imposibilidad de concretar decisiones financieras	Alto	Alto
	Coordinadora Académica	Control y seguimiento académico	Alto	Alto
	Inspectora	Control de estudiantes y docentes	Alto	Alto
	Usuarios Docentes	Interrupción en las actividades educativas	Alto	Alto
	Estudiantes	Imposibilidad de concretar las obligaciones contrac-tuales	Alto	Alto

Tabla 6.5 Valuación de activos de apoyo (Elaborado por: Investigador) (cont.)

Tabla 6.5 Valuación de activos de apoyo (cont.)

Tipo	**Activo**	**Criterio Consecuencias**	**Valuación**	**Valuación del activo**
Instalaciones	Laboratorio	Pérdida de estudiantes	Alto	Alto
		Pérdida de ventaja tecnológica	Alto	
Servicios	Servicios esenciales Energía eléctrica	Interrupción en el uso del Laboratorio	Alto	Alto
	Comunicación Teléfono Internet	Interrupción en la propia organización Pérdida de efectividad Interrupción del servicio	Alto	Alto

Tabla 6.5: Valuación de Activos de Apoyo (Elaborado por: Investigador)

6.8.2.6.6 Valoración del Impacto

La valoración del impacto se basa en la siguiente escala: Directo o Indirecto

Tipo	Activo	Criterio de valuación	Valuación del activo	Valoración del Impacto
Proceso de negocio	Formación de niños, niñas y adolescentes	Poner en peligro la seguridad de los estudiantes	Alto	Directo
		Interrupción del servicio		
		Daño de la reputación		

Tabla 6.6: Valoración del Impacto del Activo tipo Proceso de Negocio (Elaborado por: Investigador)

Valoración del impacto de activos de apoyo

Tipo	Activo	Criterio Consecuencias	Valuación final	Valoración del impacto
Hardware	Equipos fijos Computadores del Laboratorio Tics	Pérdida de la reputación	Alto	Directo
		Baja la calidad educativa		
		El valor de reemplazo final de pérdida de este activo		

Tabla 6.7: Valoración del Impacto de activos de apoyo (cont.)

Tabla 6.7: Valoración del Impacto de activos de apoyo (cont.)

Tipo	Activo	Criterio Consecuencias	Valuación final	Valoración del impacto
...	Servidor de control de acceso a Internet	Interrupción del servicio de Internet	Alto	Indirecto
Software	Licencias del Sistema Operativo	Pérdida de confianza de los padres de familia	Alto	Indirecto
		Pérdida de credibilidad		
		Pérdida en la reputación		
		Violación de leyes		
	Servicio de mantenimiento o administración del software	Costo interno adicional	Medio	Directo
		Costo financiero para emergencias o reparaciones		
		Daños materiales		
	Paquetes de software Matemáticas, Inglés Microsoft Office	Interrupción en el servicio	Medio	Indirecto
	Antivirus	Poner en peligro la seguridad de los estudiantes	Alto	Indirecto

Tabla 6.7: Valoración del Impacto de activos de apoyo (cont.)

Tabla 6.7: Valoración del Impacto de activos de apoyo (cont.)

Tipo	Activo	Criterio Consecuencias	Valuación final	Valoración del impacto
…	…	… Deterioro del rendimiento del equipo	…	…
	Navegadores para Internet	No pueden verse correctamente las páginas web	Alto	Directo
Redes	Soporte y medios Red pública	Poner en peligro la seguridad de los estudiantes Los docentes no pueden preparar sus clases utilizando material de Internet	Alto	Directo
	Ethernet Wireless 802.11 a/b/c/n/g	Interrupción del servicio de red Pérdida de competitividad	Alto	Indirecto
	Dispositivos de comunicaciones Router Switch	Formación académica de los estudiantes Preparación de material e investigación de los docentes Pérdida económica	Alto	Directo

Tabla 6.7: Valoración del Impacto de activos de apoyo (cont.)

Tabla 6.7: Valoración del Impacto de activos de apoyo (cont.)

Tipo	Activo	Criterio Consecuencias	Valuación final	Valoración del impacto
	Interfaz de comunicaciones Tarjetas de red inalámbricas Tarjetas de red Ethernet	Costo interno adicional	Alto	Directo
		Deteriora el rendimiento del laboratorio		
		Interrupción del servicio de red		
		Los estudiantes no pueden hacer uso del Internet para aprender		
Personal	Toma de decisiones Propietario – Director	Imposibilidad de concretar decisiones financieras	Alto	Directo
	Coordinadora Académica	Control y seguimiento académico	Alto	Indirecto
	Inspectora	Control de estudiantes y docentes	Alto	Indirecto
	Usuarios Docentes	Interrupción en las actividades educativas	Alto	Indirecto
	Estudiantes	Imposibilidad de concretar las obligaciones contractuales	Alto	Directo

Tabla 6.7: Valoración del Impacto de activos de apoyo (cont.)

Tabla 6.7: Valoración del Impacto de activos de apoyo (cont.)

Tipo	Activo	Criterio Consecuencias	Valuación final	Valoración del impacto
Instalacio-nes	Laboratorio	Pérdida de estudiantes	Alto	
		Pérdida de ventaja tecnológica		
Servicios	Servicios esenciales Energía eléctrica	Interrupción en el uso del Laboratorio	Alto	Indirecto
	Comunicación Teléfono Internet	Interrupción en la propia organización Pérdida de efectividad Interrupción del servicio	Alto	Indirecto

Tabla 6.7: Valoración del Impacto de los activos de apoyo (Elaborado por: Investigador)

6.8.2.6.7 Identificación de amenazas

El origen de la amenaza está basado en la siguiente tabla:

A	Accidental
D	Usada para todas las acciones deliberadas dirigidas a los activos
E	(Del medio ambiente) es relevante

Tabla 6.8: Categorías de Amenazas (Fuente: IEC/ITC ISO 27005,2008 pág. 39)
(Elaborado por: Investigador)

Identificación de amenazas

Tipo	**Amenaza**	**Origen**
Daño Físico	Fuego	A,D,E
	Accidente grave	A,D,E
	Destrucción de equipos o medios	A,D,E
	Polvo, corrosión, congelación	A,D,E
Eventos naturales	Fenómenos climáticos	E
	Fenómenos sísmicos	E
	Fenómenos volcánicos	E
	Fenómenos meteorológicos	E
	Inundaciones	E
Pérdida de servicios esenciales	Peligro del aire acondicionado o sistema de abastecimiento de agua	A,D
…	Pérdida de energía eléctrica	A,D,E
	Falla en los equipos de telecomunicaciones	A,D

Tabla 6.9 Identificación de amenazas (Fuente: IEC/ITC 27005, 2008, pág. 11, 39-41)
(Elaborado por: Investigador)(cont.)

Tabla 6.9 Identificación de amenazas (cont.)

Tipo	Amenaza	Origen
…	Robo de los medios de comunicación o documentos	D
	Robo de equipos	D
	La recuperación de los medios de comunicación reciclados o desechados	A,D
	Divulgación	A,D
	Datos de fuentes no confiables	D
	La manipulación del hardware	D
	La manipulación del software	A,D
Fallas técnicas	Daño en el equipo	A
	Malfuncionamiento del equipo	A
	Saturación del sistema de información	A,D
	Malfuncionamiento del software	A
	Incumplimiento del mantenimiento del sistema de información	A,D
Acciones no autorizadas	Uso de equipo no autorizado	D
	Copia de software fraudulento	D
	Uso de falsificación o software copiado	A,D
Funciones comprometedoras	Error en el uso	A
	Incumplimiento de la disponibilidad del personal	A,D,E
	Abuso de derechos	A,D,E

Tabla 6.9: Tipos de amenazas con su origen adaptado de la propuesta ISO 27005 (Fuente: IEC/ITC 27005, 2008, págs. 11,39-41) (Elaborado por: Investigador)

Las amenazas de origen humano se desglosan en la siguiente tabla:

Origen de la amenaza	Motivación	Posibles consecuencias
Criminal informático	Destrucción de la información Divulgación de información ilegal Ganancia de dinero Alteración de datos no autorizados	Crimen informático (acoso por intimidación, acoso para gratificación sexual, envío de fotos, videos, sonidos sin consentimiento, sexting,) a los niños, niñas y adolescentes Actos fraudulentos (reproducir, suplantación, interceptación) Soborno de información Suplantación de identidad Intrusión
Insiders (mal entrenados, descontentos, maliciosos, negligentes, deshonestos, o empleados que sean despedidos)	Curiosidad Ego Inteligencia Ganancia de dinero Venganza Errores no intencionales y omisiones (ejemplo errores al ingresar datos, errores de programación)	Asalto a un empleado Correo negro Navegación de la información confidencial Abuso del computador Fraude y robo Soborno de información Entrada de falsificados, datos corruptos Intercepción Código malicioso (Ejemplo virus, bomba lógica, Troyanos La venta de información personal Errores del sistema Intrusión. Sabotaje Acceso al sistema sin autorización

Tabla 6.10: Amenazas de origen humano adaptadas del Anexo C, Norma ISO: 27005 (Fuente: IEC/ITC 27005, 2008, págs. 11, 39-41) (Elaborado por: Investigador)

6.8.2.6.8 Identificación de controles existentes

Gráfico: 6.7 Fotografía Profesor de Tics identificando los controles existentes en el CELP (Elaborado por: Investigador)

Para el efecto se trabaja con Lic. David De La Cruz profesor de Tics de la Institución que viene a tomar el rol de "Oficial de Seguridad de la Información" y se recopila la información de la visita técnica realizada.

Tipo	Amenaza	Origen	Control					
			Tipo		Estado del control			
			Planeado	Existente	Se justifica	Inefi-ciente	No sufícien-te	No justifi cado
Daño Físico	Fuego	A,D,E		Extinguidores	X			
	Accidente grave	A,D,E			X			
	Destrucción de equipos o medios	A,D,E					X	

Tabla 6.11: Identificación de controles existentes del CELP (Fuente: IEC/ITC 27005, 2008, pág. 12) (Elaborado por: Investigador)(cont.)

Tabla 6.11: Identificación de controles existentes del CELP (cont.)

Tipo	Amenaza	Origen	Control					
			Tipo		Estado del control			
			Planeado	Existente	Se justifica	Inefi-ciente	No sufícien-te	No justifi cado
…	Polvo, corrosión	A,D,E		Mantenimiento cada inicio de clases			X	
Eventos naturales	Fenómenos climáticos	E	Dejar apagado los equipos	Plan de gestión de riesgos			X	
	Fenómenos sísmicos	E		Plan de gestión de riesgos (Anexos)	X			
	Fenómenos volcánicos	E		Plan de gestión de riesgos (Anexos)	X			
	Inundaciones	E		Plan de gestión de riesgos (Anexos)	X			
Pérdida de servicios esencia-les	Pérdida de energía eléctrica	A,D		_____			X	
	Falla en los equipos de telecomunicaciones	A,D		_____			X	
	Robo de equipos	D					X	

Tabla 6.11: Identificación de controles existentes del CELP (Fuente: IEC/ITC 27005, 2008, pág. 12) (Elaborado por: Investigador) (cont.)

Tabla 6.11: Identificación de controles existentes del CELP (cont.)

Tipo	Amenaza	Origen	Control					
			Tipo		Estado del control			
			Planeado	Existente	Se justifica	Inefi-ciente	No sufícien-te	No justifi cado
	La recuperación de los medios de comunicación reciclados o desechados	A,D			X			
	La manipulación del hardware	D			X			
	La manipulación del software	A,D		Deep Freeze	X			
Fallas técnicas	Daño en el equipo	A	Fondo pagan los padres de familia que es el fondo de mantenimi ento			X		
	Malfuncionamiento del equipo	A				X		
	Malfuncionamiento del software	A				X		

Tabla 6.11: Identificación de controles existentes del CELP (Fuente: IEC/ITC 27005, 2008, pág. 12) (Elaborado por: Investigador) (cont.)

Tabla 6.11: Identificación de controles existentes del CELP (cont.)

Tipo	Amenaza	Origen	Control					
			Tipo		Estado del control			
			Planeado	Existente	Se justifica	Inefi-ciente	No sufícien-te	No justifi cado
Acciones no autorizadas	Uso de equipo no autorizado	D			X			
	Copia de software fraudulento	D				X		
	Uso de falsificación o software copiado	A,D				X		
Funciones compro-metedoras	Error en el uso	A			X			
	Abuso de derechos	A,D			X			
	Incumplimiento de la disponibilidad del personal	A,D,E					X	

Tabla 6.11: Identificación de controles existentes del CELP (Fuente: IEC/ITC 27005, 2008, pág. 12) (Elaborado por: Investigador)

Identificación de controles existentes relacionados con el origen de la amenaza

El objetivo de este paso es identificar controles existentes y planeados.

Origen de la amenaza	Motivación	Posibles consecuencias	Control					
			Tipo		Estado del control			
			Planeado	Existente	Se justifica	Inefi-ciente	No sufícien-te	No justifi cado
Criminal informático	Destrucción de la información	Crimen informático (acoso				X		
Criminal informático	Divulgación de información ilegal Ganancia de dinero Alteración de datos no autorizados	cibernético) Actos fraudulentos (reproducir, suplantación, interceptación) Soborno de información Suplantación de identidad Intrusión				X		

Tabla 6.12: Identificación de controles existentes relacionados con origen de amenaza humana (Fuente: IEC/ITC 27005, 2008, pág. 12) (Elaborado por: Investigador)

6.8.2.6.9 Identificación de vulnerabilidades

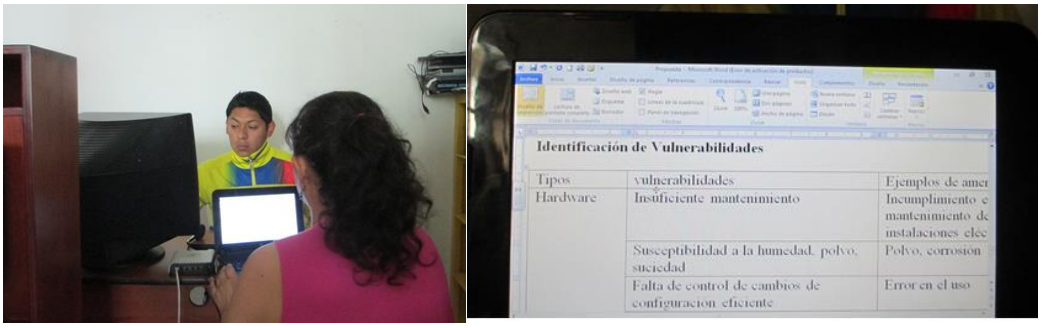


Gráfico: 6.8 Fotografía Profesor de Tics en reunión Identificando Vulnerabilidades y amenazas (Elaborado por: Investigador)

La identificación de vulnerabilidades, se genera a partir de la visita técnica realizada con la colaboración de Lic. David De La Cruz profesor de Tics de la Institución.

Tipos	Vulnerabilidades	Amenazas
Hardware	Insuficiente mantenimiento	Incumplimiento en el mantenimiento de equipos e instalaciones eléctricas
	Susceptibilidad a la humedad, polvo, suciedad	Polvo, corrosión
	Falta de control de cambios de configuración eficiente	Error en el uso
	Defectos bien conocidos en el software	Abuso de derechos
Software	Drivers sin instalar en algunas máquinas	Error en el uso
	Fechas incorrectas	Error en el uso

Tabla 6.13: Identificación de vulnerabilidades y amenazas del CELP (Fuente: IEC/ITC 27005, 2008, pág. 12) (Elaborado por: Investigador) (cont.)

Tabla 6.13: Identificación de vulnerabilidades y amenazas del CELP (cont.)

Tipos	Vulnerabilidades	Amenazas
… Softtware	Mala gestión de contraseñas freeze	Se actualiza el antivirus una vez al año cuando la persona que tiene la clave a hacer mantenimiento, nunca se actualizan los parches del Sistema Operativo.
Red	Líneas de comunicación desprotegidas (cable de teléfono desprotegido, tubería telefónica con agua)	Denegación de acciones (No haya Internet por ruptura del cable)
	Arquitectura de red insegura	Espía remoto que adivine contraseña e ingrese a la red
	Contraseña del router evidente	Espía remoto
	Inadecuada administración de la red	Conflictos de IP
Personal	Ausencia de personal	Incumplimiento de disponibilidad del personal encargado de tecnología
	Procedimientos de reclutamiento inadecuados	Destrucción de equipo o medios
	Insuficiente entrenamiento en seguridad	Error en el uso
	Incorrecto uso de software y hardware	Error en el uso
Personal	Falta de conciencia de seguridad	Error en el uso
	Falta de mecanismos de monitoreo	Procesamiento ilegal de datos

Tabla 6.13: Identificación de vulnerabilidades y amenazas del CELP CELP (Fuente: IEC/ITC 27005, 2008, pág. 12) (Elaborado por: Investigador) (cont.)

Tabla 6.13: Identificación de vulnerabilidades y amenazas del CELP (cont.)

Tipos	Vulnerabilidades	Amenazas
Sitio	Localización en un área susceptible a inundaciones	Destrucción de equipos o medios
	Insuficientes puntos de conexión eléctrica	Corto circuito, los cables están en el piso
Organización	Falta de un procedimiento para que los docentes usen el laboratorio de Tics.	Abuso de derechos o no usan los docentes para dictar clases
	Falta de procedimientos de identificación y valoración de riesgos	Abuso de derechos
	La falta de informes de fallos del Profesor de Tics	Abuso de derechos
	La falta de una adecuada asignación de responsabilidades de seguridad de la información	Denegación de acciones
	Falta de planes de continuidad	Falla en el equipo
	Falta de registros de encargado de tecnología y profesor de TICs	Error en uso
	Falta de responsabilidades de seguridad de información en descripciones de puestos de trabajo	Error en uso
	Falta de procesos disciplinarios en caso de que ocurran incidentes de la seguridad de la información	Robo de equipos
	Falta de revisiones por parte de la dirección regulares	Uso de equipos no autorizados

Tabla 6.13: Identificación de vulnerabilidades y amenazas del CELP CELP (Fuente: IEC/ITC 27005, 2008, pág. 12) (Elaborado por: Investigador) (cont.)

6.8.2.6.10 Identificación de consecuencias

Gráfico: 6.9 Fotografía con Profesor de TICs identificando consecuencias (Elaborado por: Investigador)

Las consecuencias son analizadas en términos de pérdida de confidencialidad, integridad y disponibilidad con Lic. David De La Cruz profesor de Tics de la Institución, entendiéndose cada una de ellas de la siguiente forma:

"Disponibilidad es la propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada (ISO/IEC, 13335-1:2004)" (ISO/ICE, ITC, 2005, pág. 9).

"Confidencialidad es la propiedad que esta información esté disponible y no sea divulgada a personas, entidades o procesos no – autorizados. (ISO/IEC, 13335-1:2004)" (ISO/ICE, ITC, 2005, pág. 9).

"Integridad es la propiedad de salvaguardar la exactitud e integridad de los activos. (ISO/IEC, 13335-1:2004)" (ISO/ICE, ITC, 2005, pág. 10).

A continuación se presenta una tabla con la identificación de consecuencias.

Activos	Escenario de incidente	Consecuencias operacionales						Naturaleza	
		Tiempo de reparación	Pérdida de Tiempo	Pérdida de oportuni-dades	Salud y seguridad	Costo financiero de habilidades específicas para reparar el daño o reemplazo	Imagen, reputación y buena voluntad	Tem-poral	Perma-nente
Formación de niños, niñas y adolescentes	Tendría un impacto directo en la formación de niños, niñas y adolescentes ya que puede ser afectada la integridad de los mismos al ser víctimas de alguna amenaza como crimen informático, engaños, pornografía, delincuencia, cyberbulling, cyberacoso, entre otros.				X		X		X
Equipos fijos Computadores del Laboratorio Tics	Impacto sería directo porque involucra la reposición de los mismos. En caso de que los equipos fijos del Laboratorio no están disponibles pueden perder ventaja competitiva, y sin equipos no pueden hacer uso del Internet Docentes y Estudiantes	X				X		X	
Servidor de	Impacto indirecto ya que en caso de existir	X	X				X	X	

Tabla 6.14: Escenarios de incidente con consecuencias (Fuente: IEC/ITC27005, pág12) (Elaborado: Investigador) (cont.)

Tabla 6.14: Escenarios de incidente con sus consecuencias (cont.)

Activos	Escenario de incidente	Consecuencias operacionales						Naturaleza	
		Tiempo de reparación	Pérdida de Tiempo	Pérdida de oportuni-dades	Salud y seguridad	Costo financiero de habilidades específicas para reparar el daño o reemplazo	Imagen, reputación y buena voluntad	Tem-poral	Perma-nente
…	…	…	…	…	…	…	…	…	…
control de acceso a Internet	eliminación o manipulación de logs de páginas de navegación afecta a la integridad y confidencialidad del mismo. Si no está disponible no pueden navegar en Internet y se bloquea el acceso a Internet								
Sistema Operativo	El no disponer de licencias afecta a la imagen de la Institución. La integridad se ve afectada ya que un software pirata es vulnerable a instalación de código						X	X	

Tabla 6.14: Escenarios de incidente con sus consecuencias(Fuente:IEC/ITC27005, pág.12)(Elaborado: Investigador)(cont.)

Tabla 6.14: Escenarios de incidente con sus consecuencias (cont.)

Activos	Escenario de incidente	Consecuencias operacionales						Naturaleza	
		Tiempo de reparación	Pérdida de Tiempo	Pérdida de oportuni-dades	Salud y seguridad	Costo financiero de habilidades específicas para reparar el daño o reemplazo	Imagen, reputación y buena voluntad	Tem-poral	Perma-nente
…	malicioso, virus, entre otros, por ende no es confiable tener un sistema operativo sin licencia ya que pueden realizar los propietarios una visita y la Institución entrar en problemas legales y multas fuertes	…	…	…	…	…	…	…	…
Servicio de mantenimiento o administración del software	Impacto directo ya que pueden dañarse el software y la institución incurriría en gastos económicos. Si el servicio del mantenimiento o administración de software no está disponible cuando la Institución lo requiera no recibe actualizaciones lo que implica que sea vulnerable a virus, código malicioso, entre	X						X	

Tabla 6.14:Escenarios de incidente con sus consecuencias(Fuente: IEC/ITC27005, pág.12)(Elaborado: Investigador)(cont.)

Tabla 6.14: Escenarios de incidente con sus consecuencias (cont.)

Activos	Escenario de incidente	Consecuencias operacionales						Naturaleza	
		Tiempo de reparación	Pérdida de Tiempo	Pérdida de oportuni-dades	Salud y seguridad	Costo financiero de habilidades específicas para reparar el daño o reemplazo	Imagen, reputación y buena voluntad	Tem-poral	Perma-nente
…	otros; y al no haber actualizaciones la confidencialidad e integridad se pierde ya que los fabricantes pueden sacar parches de corrección de errores.	…	…	…	…	…	…	…	…
Paquetes de software Matemáticas, Inglés Microsoft Office	Impacto indirecto ya que la mayoría del software educativo es libre, entonces puede instalarlo	X						X	
Antivirus	Impacto directo ya que se incurriría en costos por reparación de equipos infectados. En cuanto a disponibilidad si un antivirus no	X				X		X	

Tabla 6.14: Escenarios de incidente con sus consecuencias(Fuente: IEC/ITC 27005, 2008) (Elaborado: Investigador)(cont.)

Tabla 6.14: Escenarios de incidente con sus consecuencias (cont.)

Activos	Escenario de incidente	Consecuencias operacionales						Naturaleza	
		Tiempo de reparación	Pérdida de Tiempo	Pérdida de oportuni-dades	Salud y seguridad	Costo financiero de habilidades específicas para reparar el daño o reemplazo	Imagen, reputación y buena voluntad	Tem-poral	Perma-nente
	está instalado y actualizado se puede incurrir en infección de virus lo que afecta la integridad del equipo, la confidencialidad en el uso de información. En el uso de Internet es susceptible a descargas de virus.								
Navegadores para Internet	Impacto indirecto ya que los estudiantes pueden hacer uso del navegador pero no en óptimas condiciones, y no involucra costos adicionales. Afecta la confidencialidad y la integridad en caso de que se hayan metido virus por falta de actualización y se baje código malicioso.		X	X				X	

Tabla 6.14: Escenarios de incidente con sus consecuencias (Fuente: IEC/ITC 27005, 2008, pág. 12) (Elaborado por: Investigador) (cont.)

Tabla 6.14: Escenarios de incidente con sus consecuencias (cont.)

Activos	Escenario de incidente	Consecuencias operacionales						Naturaleza	
		Tiempo de reparación	Pérdida de Tiempo	Pérdida de oportuni-dades	Salud y seguridad	Costo financiero de habilidades específicas para reparar el daño o reemplazo	Imagen, reputación y buena voluntad	Tem-poral	Perma-nente
Medios Ethernet, Wireless 802.11 a/b/c/n/g	Impacto directo ya que afecta a la imagen de la institución En el caso de no estar disponible los estudiantes no tendrían Internet en el Laboratorio y los profesores tampoco						X	X	
Dispositivos de comunicaciones Router Switch	Impacto indirecto ya que el costo sería la interrupción del servicio de Internet y de la Red. Afecta a la integridad y confidencialidad de los computadores, servidor ya que al no tener Internet no se actualiza el software incluyendo el antivirus	X	X			X	X		X

Tabla 6.14: Escenarios de incidente con sus consecuencias CELP (Fuente: IEC/ITC 27005, 2008, pág. 12) (Elaborado por: Investigador) (cont.)

Tabla 6.14: Escenarios de incidente con sus consecuencias (cont.)

Activos	Escenario de incidente	Consecuencias operacionales						Naturaleza	
		Tiempo de reparación	Pérdida de Tiempo	Pérdida de oportuni-dades	Salud y seguridad	Costo financiero de habilidades específicas para reparar el daño o reemplazo	Imagen, reputación y buena voluntad	Tem-poral	Perma-nente
Interfaz de comunicaciones Tarjetas de red inalámbricas Tarjetas de red Ethernet	Impacto indirecto pues el costo involucra la interrupción del servicio de red e Internet. Afecta a la integridad y confidencialidad de los computadores, servidor ya que al no tener Internet no se actualiza el software incluyendo el antivirus	X				X		X	
Toma de decisiones Propietario – Director	Impacto directo ya que es la persona que toma decisiones y nada que involucre lo económico fluye si no es aprobado por el Propietario.	X		X				X	

Tabla 6.14: Escenarios de incidente con sus consecuencias CELP (Fuente: IEC/ITC 27005, 2008, pág. 12) (Elaborado por: Investigador) (cont.)

Tabla 6.14: Escenarios de incidente con sus consecuencias (cont.)

Activos	Escenario de incidente	Consecuencias operacionales						Naturaleza	
		Tiempo de reparación	Pérdida de Tiempo	Pérdida de oportuni-dades	Salud y seguridad	Costo financiero de habilidades específicas para reparar el daño o reemplazo	Imagen, reputación y buena voluntad	Tem-poral	Perma-nente
	Afecta a la Integridad ya que generalmente no pasa en la Institución y mientras tanto no se puede solucionar los inconvenientes, no hay acceso a la oficina donde está el servidor con el sistema de información de la institución.								
Estudian-tes	Impacto es directo si no hay estudiantes, ya que afecta económicamente a la Institución.						X		X
Laboratorio de Tics	Impacto directo pues habría pérdida de ventaja competitiva, los estudiantes no estarían a la par con el Internet y los avances tecnológicos; lo que podría conllevar la disminución de estudiantes, por ende disminución de ingresos						X	X	

Tabla 6.14: Escenarios de incidente con sus consecuencias CELP (Fuente: IEC/ITC 27005, 2008, pág.12) (Elaborado por: Investigador) (cont.)

Tabla 6.14: Escenarios de incidente con sus consecuencias (cont.)

Activos	Escenario de incidente	Consecuencias operacionales						Naturaleza	
		Tiempo de reparación	Pérdida de Tiempo	Pérdida de oportuni-dades	Salud y seguridad	Costo financiero de habilidades específicas para reparar el daño o reemplazo	Imagen, reputación y buena voluntad	Tem-poral	Perma-nente
Servicios esenciales Energía eléctrica	Impacto indirecto, depende de proveedores; en el caso de la Institución tiene jornada matutina y aulas bien iluminadas. Afectaría la disponibilidad del uso del Laboratorio de Tics y por ende de Internet Con respecto a la Integridad y confidencialidad, si hay un corte puede afectar en daños del software del servidor y computadores ya que no tienen un UPS para apagar correctamente los mismos	…	X	…	…	…	X	X	…
Comunica-ción Teléfono Internet	Impacto indirecto, interfiere en el uso de Internet en cuanto a la disponibilidad y se depende de los proveedores para la reparación de los mismos. La Integridad y Confidencialidad no afecta		X					X	

Tabla 6.14: Escenarios de incidente con sus consecuencias CELP (Fuente: IEC/ITC 27005, 2008, pág. 13) (Elaborado por: Investigador) (cont.)

6.8.2.6.11 Estimación del riesgo

Valoración de consecuencias

La valoración de consecuencias de un incumplimiento de seguridad de información se realiza en base a pérdida de confidencialidad, integridad o disponibilidad de los activos, para lo cual se ha establecido una escala del 0 al 3 como se puede observar en la siguiente tabla.

Confidencialidad	Integridad	Disponibilidad
0 Nada grave	0 Nada grave	0 Nada grave
1 Poco grave	1 Poco grave	1 Poco grave
2 Grave	2 Grave	2 Grave
3 Muy Grave	3 Muy Grave	3 Muy Grave

Tabla 6.15: Escala de Valoración de consecuencias en base a confidencialidad, integridad y disponibilidad (Elaborado por: Investigador)

A continuación se presenta una tabla con la valoración de consecuencias, descrita por activos, escenario de incidente, consecuencia operacional, criterio de impacto (valoración de reemplazo del activo del CELP, consecuencia por la pérdida de compromiso con los activos del CELP").

Activos	Escenario de incidente	Consecuencia operacional	Criterio de Impacto	
			Valoración de reemplazo del activo	**Consecuencias para el CELP por la pérdida o compromiso de los activos**
Formación de niños, niñas y adolescentes	La formación de niños, niñas y adolescentes puede ser afectada en la integridad, al ser víctimas de alguna amenaza como crimen informático, engaños, pornografía, delincuencia, cyberbulling, cyberacoso, entre otros.	Salud y seguridad Imagen, reputación y buen nombre	No tiene reemplazo	Conf: 3 / Integ: 3 / Disp: 0
Equipos fijos Computadores del Laboratorio Tics	Impacto sería directo porque involucra la reposición de los mismos En caso de que los equipos fijos del Laboratorio no están disponibles pueden perder ventaja competitiva, y sin equipos no pueden hacer uso del Internet Docentes y Estudiantes	Tiempo de reparación Costo financiero de habilidades específicas para reparar el daño o reemplazo	$ 450	Conf: / Integ: 2 / Disp: 3

Tabla 6.16: Escenarios de incidente con su consecuencia operacional y criterio de impacto (Fuente: IEC/ITC 27005, 2008, págs. 14,15) (cont.)

Tabla 6.16: Escenarios de incidente con su consecuencia operacional y criterio de impacto (cont.)

Activos	**Escenario de incidente**	**Consecuencia operacional**	**Criterio de Impacto**	
			Valoración de reemplazo del activo	**Consecuencias para el CELP por la pérdida o compromiso de los activos**
Servidor de control de acceso a Internet	Eliminación o manipulación de logs de páginas de navegación afecta a la integridad y confidencialidad del mismo. Si no está disponible no pueden navegar en Internet y se bloquea el acceso a Internet para estudiantes y docentes.	Tiempo de reparación; pérdida de tiempo; imagen; reputación y buena voluntad	Arreglo $ 100 Reemplazo $ 600	Conf: 2 / Integ: 2 / Disp: 2
Sistema Operativo	El no disponer de licencias afecta a la imagen de la Institución. La integridad se ve afectada ya que un software pirata es vulnerable a instalación de código malicioso, virus, entre otros Por ende no es confiable tener un sistema operativo sin licencia ya que el CELP entrar en problemas legales y multas fuertes	Imagen, reputación y buen nombre del Centro Educativo	$ 8500	Conf: 3 / Integ: 3 / Disp: 3

Tabla 6.16: Escenarios de incidente con su consecuencia operacional y criterio de impacto (Fuente: IEC/ITC 27005, 2008, págs. 14,15) (cont.)

Tabla 6.16: Escenarios de incidente con su consecuencia operacional y criterio de impacto (cont.)

Activos	**Escenario de incidente**	**Consecuencia operacional**	**Criterio de Impacto**	
			Valoración de reemplazo del activo	**Consecuencias para el CELP por la pérdida o compromiso de los activos**
Servicio de mantenimiento o administración del software	Impacto directo ya que pueden dañarse el software y la institución incurriría en gastos económicos. Si el servicio del mantenimiento o administración de software no está disponible cuando la Institución lo requiera no recibe actualizaciones lo que implica que sea vulnerable a virus, código malicioso, entre otros; y al no haber actualizaciones la confidencialidad e integridad se pierde ya que los fabricantes pueden sacar parches de corrección de errores.	Tiempo de reparación	$30 por equipo	Conf: 1 / Integ: 1 / Disp: 3
Antivirus	Impacto directo ya que se incurriría en costos por reparación de equipos infectados. La disponibilidad, afecta con infección de virus por falta de actualización.	Tiempo de reparación Costo financiero de	3 horas $120	Conf: 3 / Integ: 2 / Disp: 2

Tabla 6.16: Escenarios de incidente con su consecuencia operacional y criterio de impacto (Fuente: IEC/ITC 27005, 2008, págs. 14,15) (Elaborado por: Investigador) (cont.)

Tabla 6.16: Escenarios de incidente con su consecuencia operacional y criterio de impacto (cont.)

Activos	**Escenario de incidente**	**Consecuencia operacional**	**Criterio de Impacto**	
			Valoración de reemplazo del activo	**Consecuencias para el CELP por la pérdida o compromiso de los activos**
… Antivirus	… Descargas de virus desde Internet.	… habilidades específicas para reparar el daño o reemplazo	…	…
Navegadores para Internet	Impacto indirecto ya que los estudiantes pueden hacer uso del navegador pero no en óptimas condiciones, y no involucra costos adicionales. Afecta la confidencialidad y la integridad en caso de que se hayan metido virus por falta de actualización y se baje código malicioso, y después de ello va ligado la disponibilidad del activo	Tiempo de reparación Pérdida de Tiempo	2h30 en actualizar en todo el Laborato-rio	Conf: 3 Integ: 2 Disp: 2

Tabla 6.16: Escenarios de incidente con su consecuencia operacional y criterio de impacto (Fuente: IEC/ITC 27005, 2008, págs. 14,15) (cont.)

Tabla 6.16: Escenarios de incidente con su consecuencia operacional y criterio de impacto (cont.)

Activos	**Escenario de incidente**	**Consecuencia operacional**	**Criterio de Impacto**	
			Valoración de reemplazo del activo	**Consecuencias para el CELP por la pérdida o compromiso de los activos**
Medios Red Ethernet, Red inalámbrica 802.11 a/b/c/n/g	Impacto directo ya que afecta a la imagen de la institución En el caso de no estar disponible los estudiantes no tendrían Internet en el Laboratorio y los profesores tampoco podrán hacer uso de este para preparar sus clases, o si no está disponible el Sistema de Información cuando llegan a solicitar reportes autoridades o padres de familia, de información actual o histórica, no pueden ingresar al Sistema en secretaría. No existe autenticación en la red inalámbrica. Clave router wireless insegura. Direccionamiento IP de los equipos del área administrativa sin orden.	Imagen, reputación y buen nombre.	No tiene precio	Conf: 2 / Integ: 3 / Disp: 3

Tabla 6.16: Escenarios de incidente con su consecuencia operacional y criterio de impacto (Fuente: IEC/ITC 27005, 2008, págs. 14,15) (Elaborado por: investigador) (cont.)

Tabla 6.16: Escenarios de incidente con su consecuencia operacional y criterio de impacto (cont.)

Activos	**Escenario de incidente**	**Consecuencia operacional**	**Criterio de Impacto**	
			Valoración de reemplazo del activo	**Consecuencias para el CELP por la pérdida o compromiso de los activos**
Red ethernet	Switch y servidor ubicado en un lugar que pasa cerrado y únicamente tiene acceso una persona que no pasa en la Institución todo el día, por ende no está disponible la red Ethernet, y por ende el acceso a Internet de personal administrativo y docente. Tienen 2 redes planas separadas, lo que a la larga impedirá el crecimiento tecnológico.	…	…	…
Dispositivos de comunica-ciones Router Switch	Impacto indirecto ya que el costo sería la interrupción del servicio de Internet y de la Red. Afecta a la integridad y confidencialidad de los computadores, servidor ya que al no tener Internet no se actualiza el software incluyendo el antivirus	Tiempo de reparación, pérdida de Tiempo, Costo financiero de	Indeter-minado Reem-plazo $ 800	Conf: 0 / Integ: 2 / Disp: 3

Tabla 6.16: Escenarios de incidente con su consecuencia operacional y criterio de impacto (Fuente: IEC/ITC 27005, 2008, págs. 14,15)(Elaborado por: Investigador) (cont.)

Tabla 6.16: Escenarios de incidente con su consecuencia operacional y criterio de impacto (cont.)

<table>
<tr><th rowspan="2">Activos</th><th rowspan="2">Escenario de incidente</th><th rowspan="2">Consecuencia operacional</th><th colspan="2">Criterio de Impacto</th></tr>
<tr><th>Valoración de reemplazo del activo</th><th>Consecuencias para el CELP por la pérdida o compromiso de los activos</th></tr>
<tr><td>…</td><td>…</td><td>habilidades específicas para reparar el daño o reemplazo
Imagen, reputación y buena voluntad</td><td>…</td><td>…</td></tr>
<tr><td>Interfaz de comunicaciones
Tarjetas de red inalámbricas
Tarjetas de red Ethernet</td><td>Impacto indirecto pues el costo involucra la interrupción del servicio de red e Internet.
Afecta a la integridad y confidencialidad de los computadores, servidor ya que al no tener Internet no se actualiza el software incluyendo el antivirus</td><td>Tiempo de reparación
Costo financiero de habilidades específicas para reparar el daño o reemplazo</td><td>$ 20 dólares cada tarjeta</td><td><table><tr><td>Conf</td><td>Integ</td><td>Disp</td></tr><tr><td>0</td><td>3</td><td>3</td></tr></table></td></tr>
</table>

Tabla 6.16: Escenarios de incidente con su consecuencia operacional y criterio de impacto (Fuente: IEC/ITC 27005, 2008, págs. 14,15) (cont.)

Tabla 6.16: Escenarios de incidente con su consecuencia operacional y criterio de impacto (cont.)

Activos	**Escenario de incidente**	**Consecuencia operacional**	**Criterio de Impacto**	
			Valoración de reemplazo del activo	**Consecuencias para el CELP por la pérdida o compromiso de los activos**
Toma de decisiones Propietario – Director	Impacto directo ya que es la persona que toma decisiones y nada que involucre lo económico fluye si no es aprobado por el Propietario. Afecta a la Integridad ya que generalmente no pasa en la Institución y mientras tanto no se puede solucionar los inconvenientes, no hay acceso a la oficina donde está el servidor con el sistema de información de la institución.	Tiempo de reparación Pérdida de Tiempo	No tiene precio	Conf: 3 Integ: 3 Disp: 3
Estudiantes	Impacto es directo, si no hay estudiantes, afecta económicamente a la Institución. Deseo de descubrir hace que puedan mirar imágenes no aptas para su edad, curiosidad tecnológica. Tiempo excesivo de juego en Internet	Imagen, reputación y buen nombre	No tiene precio	Conf: 3 Integ: 3 Disp: 3

Tabla 6.16: Escenarios de incidente con su consecuencia operacional y criterio de impacto (Fuente: IEC/ITC 27005, 2008, págs. 14,15) (Elaborado por: Investigador) (cont.)

Tabla 6.16: Escenarios de incidente con su consecuencia operacional y criterio de impacto (cont.)

Activos	**Escenario de incidente**	**Consecuencia operacional**	**Criterio de Impacto**	
			Valoración de reemplazo del activo	**Consecuencias para el CELP por la pérdida o compromiso de los activos**
Laboratorio de TICs	Impacto directo pues habría pérdida de ventaja competitiva, los estudiantes no estarían a la par con el avance tecnológico e Internet; lo que podría conllevar la disminución de estudiantes, por ende disminución de ingresos.	Imagen, reputación y buen nombre	$8000 si todo el Laboratorio se daña	Conf: 3, Integ: 3, Disp: 3
Servicios esenciales Energía eléctrica	Impacto indirecto, depende de proveedores; en el caso de la Institución tiene jornada matutina y aulas bien iluminadas. Afectaría la disponibilidad del uso del Laboratorio de Tics y por ende de Internet. Con respecto a la Integridad y confidencialidad, si hay un corte puede afectar en daños del software del servidor, base de datos y computadores ya que no tienen un UPS para apagar correctamente los mismos.	Pérdida de Tiempo	Pago mensual restado por el cálculo del tiempo de corte	Conf: 3, Integ: 3, Disp: 3

Tabla 6.16: Escenarios de incidente con su consecuencia operacional y criterio de impacto (Fuente: IEC/ITC 27005, 2008, págs. 14,15) (Elaborado por: Investigador) (cont.)

Tabla 6.16: Escenarios de incidente con su consecuencia operacional y criterio de impacto (cont.)

Activos	**Escenario de incidente**	**Consecuencia operacional**	**Criterio de Impacto**	
			Valoración de reemplazo del activo	**Consecuencias para el CELP por la pérdida o compromiso de los activos**
Comunica-ción Teléfono Internet	Impacto indirecto, interfiere en el uso de Internet en cuanto a la disponibilidad y se depende de los proveedores para la reparación de los mismos y los datos del sistema que son publicados en la página web no estarían disponibles. Con respecto a la Integridad y Confidencialidad, podría afectar a los datos que se están transfiriendo en la réplica para la base de datos hospedada en el host.	Pérdida de Tiempo	Pago de servicio sin usar $ 256 Pago de servicio Internet sin usar $216	Conf: 2 / Integ: 2 / Disp: 3

Tabla 6.16: Escenarios de incidente con su consecuencia operacional y criterio de impacto (Fuente: IEC/ITC 27005, 2008, págs. 14,15) (Elaborado por: Investigador)

Evaluación de la Probabilidad de incidentes

Activos	Escenario de incidente		Consecuencia 0 Nada grave 1 Poco grave 2 Grave 3 Muy Grave	Controles existentes y planificados			Probabilidad		
	Amenaza	Vulnerabilidad		Eficacia	Imple-mentación	Estado	Frecuencia de amenaza	Facilidad con que la vulnerabilidad puede ser explo-tada:Difícil Fácil- Muy Fácil	Resultado de la Pro-babilidad: Muy baja, Baja Media, Alta,Muy alta
Formación de niños, niñas y adolescentes	Acoso intimidación	Control de acceso a Internet	**Operacional** Salud y seguridad Imagen, reputación y buen nombre **Valoración** No tiene reemplazo **Pérdida de compromiso de los activos** Conf 3 / Integ 3 / Disp 0 **Impacto** Organizacional. Directo	Bajo	No	No sufí-ciente	19/100 Ver anexo 13	Muy fácil	Baja
	Acoso para gratificación sexual			Bajo	No	No sufí-ciente	8/100 Ver anexo 13	Muy Fácil	Baja
	Han enviado fotos, videos, sonidos de una persona sin su consentí-miento			Bajo	No	No sufí-ciente	30/100 Ver anexo 13	Muy fácil	Media

Tabla 6.17: Evaluación de la Probabilidad de incidentes (Fuente: IEC/ITC 27005, 2008, pág. 15) (Elaborado por: Investigador) (cont.)

Tabla 6.17: Evaluación de la probabilidad de incidentes (cont.)

Activos	**Escenario de incidente**		**Consecuencia** **0 Nada grave** **1 Poco grave** **2 Grave** **3 Muy Grave**	**Controles existentes y planificados**			**Probabilidad**		
	Amenaza	**Vulnerabilidad**		**Eficacia**	**Imple-mentación**	**Estado**	**Frecuencia de amenaza**	**Facilidad con que la vulnerabilidad puede ser explo-tada:Difícil Fácil- Muy Fácil**	**Resultado de la Pro-babilidad: Muy baja, Baja Media, Alta,Muy alta**
… Formación de niños, niñas y adolescentes	Sexting	…	…	Bajo	No	No sufí-ciente	21/100 Ver Anex13	Fácil	Baja
	Utilización de la identidad personal por parte de otra persona			Bajo	No	No sufí-ciente	22/100 Ver anexo 13	Fácil	Baja
Equipos fijos Computadores del Laboratorio Tics	Polvo, corrosión,	Falta de aseo en donde están los CPUs puede causar mal fun cionamiento en los componen-tes electrónicos	**Operacional** Tiempo de reparación, costo financiero de habilidades específicas para reparar el daño o reemplazo **Valoración** $450 mantenimiento del hardware, reemplazo de periféricos por cada equipo: Teclado $12, Mouse $ 7,Audífonos $9	Bajo	No	No sufí-ciente	1/10	Difícil	Media

Tabla 6.17: Evaluación de la Probabilidad de incidentes (Fuente: IEC/ITC 27005, 2008, págs. 14,15) (Elaborado por: Investigador) (cont.)

Tabla 6.17: Evaluación de la probabilidad de incidentes (cont.)

Activos	**Escenario de incidente**		**Consecuencia** **0 Nada grave** **1 Poco grave** **2 Grave** **3 Muy Grave**	**Controles existentes y planificados**			**Probabilidad**		
	Amenaza	**Vulnerabilidad**		**Eficacia**	**Imple-mentación**	**Estado**	**Frecuencia de amenaza**	**Facilidad con que la vulnerabilidad puede ser explo-tada:Difícil Fácil- Muy Fácil**	**Resultado de la Pro-babilidad: Muy baja, Baja Media, Alta,Muy alta**
…	…	…	…	…	…	…	…	…	…
Equipos fijos Computadores del Laboratorio Tics	Polvo, corrosión,	Falta de aseo en donde están los CPUs puede causar mal funciona-miento en los componentes electrónicos	Pérdida de los Equipos por sobrecarga o incendio Equipos: $ 8000 Bienes muebles: $ 1200 Por inexistencia de UPS Reinstalación de Software $30 por equipo **Pérdida de compromiso de los activos** Conf | Integ | Disp 0 | 2 | 3 **Impacto** Directo						

Tabla 6.17: Evaluación de la Probabilidad de incidentes(Fuente: IEC/ITC 27005, 2008, págs. 14,15) (Elaborado por: Investigador) (cont.)

Tabla 6.17: Evaluación de la probabilidad de incidentes (cont.)

Activos	**Escenario de incidente**		**Conse-cuencia** **0 Nada grave 1 Poco grave 2 Grave 3 Muy Grave**	**Controles existentes y planificados**			**Probabilidad**		
	Amenaza	**Vulnerabilidad**		**Eficacia**	**Imple-men-tación**	**Estado**	**Frecuencia de amenaza**	**Facilidad con que la vulnerabilidad puede ser explo-tada:Difícil Fácil- Muy Fácil**	**Resultado de la Pro-babilidad: Muy baja, Baja Media, Alta,Muy alta**
…	Daño de periféricos	Utilización poco cuidadosa de los periféricos	…	Bajo	Si	Inefi-ciente	10 de 15 audífonos están dañados	Muy Fácil	Alta
Equipos fijos	Abuso de derechos	Falta de informe de fallos, del Profesor de Tics		Bajo	No	Inefi-ciente	3/10	Fácil	Media
Computadores del Laboratorio Tics	Incendio	Cables en el piso, los estudiantes les pisan al sentarse o cambiar se de sitio		Media	Si	Inefi-ciente	Los incendios producidos por la electricidad son, la segunda causa conocida de incendios. (Quantum Ignis, 2013, págs. 1-2)	Muy fácil	Alta
Equipos fijos Computadores del Laboratorio Tics	Sobre-carga eléctrica	Cables eléctricos y cortapicos conectados uno a continuación de otro para abastecer las tomas eléctricas de los 15 computadores	…	Baja	Si	Inefi-ciente	Los incendios producidos por la electricidad son, la segunda causa conocida de incendios. (Quantum Ignis, 2013, págs. 1-2)	Muy fácil	Alta

Tabla 6.17: Evaluación de la Probabilidad de incidentes (Fuente: IEC/ITC 27005, 2008, págs. 14,15) (Elaborado por: Investigador) (cont.)

Tabla 6.17: Evaluación de la probabilidad de incidentes (cont.)

<table>
<tr><th rowspan="2">Activos</th><th colspan="2">Escenario de incidente</th><th rowspan="2">Consecuencia

0 Nada grave
1 Poco grave
2 Grave
3 Muy Grave</th><th colspan="3">Controles existentes y planificados</th><th colspan="3">Probabilidad</th></tr>
<tr><th>Amenaza</th><th>Vulnerabilidad</th><th>Eficacia</th><th>Imple-men-tación</th><th>Estado</th><th>Frecuencia de amenaza</th><th>Facilidad con que la vulnerabilidad puede ser explo-tada:Difícil Fácil- Muy Fácil</th><th>Resultado de la Pro-babilidad: Muy baja, Baja Media, Alta,Muy alta</th></tr>
<tr><td>Servidor de control de acceso a Internet</td><td>Abuso de derechos</td><td>Eliminación del log al reiniciar el computador por el Deep Freeze instalado.

No respaldar el log</td><td>Operacional
Tiempo de reparación
Pérdida de Tiempo
Imagen, reputación y buena voluntad
Valoración
Arreglo
$ 100
Reemplazo
$ 600
Pérdida de compromiso de los activos
<table><tr><td>Conf</td><td>Integ</td><td>Disp</td></tr><tr><td>2</td><td>2</td><td>2</td></tr></table>Impacto Directo</td><td>Baja</td><td>No</td><td>Inefi-ciente</td><td>5/5
Ver anexo 15</td><td>Muy Fácil</td><td>Muy alta</td></tr>
</table>

Tabla 6.17: Evaluación de la Probabilidad de incidentes (Fuente: IEC/ITC 27005, 2008, págs. 14,15) (Elaborado por: Investigador) (cont.)

Tabla 6.17: Evaluación de la Probabilidad de incidentes (cont.)

<table>
<tr><th rowspan="2">Activos</th><th colspan="2">Escenario de incidente</th><th rowspan="2">Consecuencia

0 Nada grave
1 Poco grave
2 Grave
3 Muy Grave</th><th colspan="3">Controles existentes y planificados</th><th colspan="3">Probabilidad</th></tr>
<tr><th>Amenaza</th><th>Vulnerabilidad</th><th>Eficacia</th><th>Imple-mentación</th><th>Estado</th><th>Frecuencia de amenaza</th><th>Facilidad con que la vulnerabilidad puede ser explo-tada:Difícil Fácil- Muy Fácil</th><th>Resultado de la Pro-babilidad: Muy baja, Baja Media, Alta,Muy alta</th></tr>
<tr><td>Sistema Operativo y Microsoft Office</td><td>Copia de software fraudulento</td><td>Licencias de uso, y por ende el software pirata es vulnerable a instalación de código malicioso, virus, entre otros</td><td>Operacional: Imagen, reputación y buen nombre del CELP
Valoración $8500
Pérdida de compromiso de los activos<table><tr><td>Conf</td><td>Integ</td><td>Disp</td></tr><tr><td>3</td><td>3</td><td>3</td></tr></table>Impacto Directo</td><td>Baja</td><td>No</td><td>Inefi-ciente</td><td>10 juicios en el año 2011</td><td>Muy fácil</td><td>Muy baja</td></tr>
<tr><td>Servicio de manteni-miento o administra-ción del software</td><td>Virus, código malicioso</td><td>Cortes de Internet frecuentes.
Partición D del disco ya que la C se encuentra protegida con el freeze</td><td>Operacional: Tiempo de reparación
Valoración $30 por equipo
Pérdida de compromiso de los activos<table><tr><td>Conf</td><td>Integ</td><td>Disp</td></tr><tr><td>1</td><td>1</td><td>3</td></tr></table>Impacto Directo</td><td>Baja</td><td>No</td><td>Inefi-ciente</td><td>5/5</td><td>Fácil</td><td>Muy alta</td></tr>
</table>

Tabla 6.17: Evaluación de la Probabilidad de incidentes (Fuente: IEC/ITC 27005, 2008, págs. 14,15) (Elaborado por: Investigador) (cont.)

Tabla 6.17: Evaluación de la Probabilidad de incidentes (cont.)

Activos	**Escenario de incidente**		**Consecuencia** **0 Nada grave** **1 Poco grave** **2 Grave** **3 Muy Grave**	**Controles existentes y planificados**			**Probabilidad**		
	Amenaza	**Vulnerabilidad**		**Eficacia**	**Imple-men-tación**	**Estado**	**Frecuencia de amenaza**	**Facilidad con que la vulnerabilidad puede ser explo-tada:Difícil Fácil- Muy Fácil**	**Resultado de la Pro-babilidad: Muy baja, Baja Media, Alta,Muy alta**
Deep Freeze	Mal funciona - miento del software	No entrega la clave al profesor de Tics por ende no se actualiza antivirus ni software	**Operacional:** Tiempo de reparación **Valoración:**$30 por equipo si se mete virus por no dejar congelado el Deep Freeze **Pérdida de compromiso de los activos** Conf 3 / Integ 3 / Disp 3 **Impacto** Indirecto	Alta	Si	Justifica	15/15	Muy fácil	Muy alta
Antivirus	Incumpli-miento en el manteni-miento del software del antivirus	Antivirus caducado y también no se actualiza la base de datos de virus por el Deep freeze instalado.	**Operacional** Tiempo de reparación Costo financiero de habilidades específicas para reparar el daño o reemplazo **Valoración:** $30 dólares por equipo **Pérdida de compromiso de los activos** Conf 3 / Integ 2 / Disp 2 **Impacto** Directo	Baja	No	Inefi-ciente	5/5	Fácil	Alta

Tabla 6.17: Evaluación de la Probabilidad de incidentes (Fuente: IEC/ITC 27005, 2008, págs. 14,15) (Elaborado por: Investigador) (cont.)

Tabla 6.17: Evaluación de la Probabilidad de incidentes (cont.)

Activos	**Escenario de incidente**		**Consecuencia** **0 Nada grave** **1 Poco grave** **2 Grave** **3 Muy Grave**	**Controles existentes y planificados**			**Probabilidad**		
	Amenaza	**Vulnerabilidad**		**Eficacia**	**Implementación**	**Estado**	**Frecuencia de amenaza**	**Facilidad con que la vulnerabilidad puede ser explotada:Difícil Fácil- Muy Fácil**	**Resultado de la Probabilidad: Muy baja, Baja Media, Alta,Muy alta**
Navegadores para Internet	Código malicioso	Software de navegadores se actualiza y se elimina la actualización al reiniciar el equipo por el deep Freeze.	**Operacional:** Tiempo de reparación, pérdida de Tiempo **Valoración:** $50 por 2h30 que se demora en quitar el deep freez, reiniciar, poner a actualizar, colocar el deep freeze, reiniciar **Pérdida de compromiso de los activos** Conf: 3 | Integ: 2 | Disp: 2 Impacto indirecto	Media	No	Inefi-ciente	20/20	Muy fácil	Muy alta
Red Ethernet, Red inalámbrica 802.11 a/b/c/n/g	Incumpli-miento de disponibi-lidad	Switch ubicado en un área donde no se prende si no llega el propietario. Inadecuada administración de la red.	**Operacional** Imagen, reputación y buen nombre. **Valoración** No tiene precio	Bajo	No	Inefi-ciente	5/7	Muy fácil	Alta

Tabla 6.17: Evaluación de la Probabilidad de incidentes (Fuente: IEC/ITC 27005, 2008, págs. 14,15) (Elaborado por: Investigador) (cont.)

Tabla 6.17: Evaluación de la Probabilidad de incidentes (cont.)

<table>
<tr><th rowspan="2">Activos</th><th colspan="2">Escenario de incidente</th><th rowspan="2">Consecuencia

0 Nada grave
1 Poco grave
2 Grave
3 Muy Grave</th><th colspan="3">Controles existentes y planificados</th><th colspan="3">Probabilidad</th></tr>
<tr><th>Amena-za</th><th>Vulnerabilidad</th><th>Eficacia</th><th>Imple-men-tación</th><th>Estado</th><th>Frecuencia de amenaza</th><th>Facilidad con que la vulnerabilidad puede ser explo-tada:Difícil Fácil- Muy Fácil</th><th>Resultado de la Pro-babilidad: Muy baja, Baja Media, Alta,Muy alta</th></tr>
<tr><td>…
Red Ethernet,

Red inalámbrica 802.11 a/b/c/n/g</td><td>Conflictos IP
Arquitectura de red inadecuada</td><td>Direccionamiento IP de los equipos del área administrativa sin orden.
Tienen 2 redes planas separadas, lo que a la larga impedirá el crecimiento tecnológico.</td><td>Pérdida de compromiso de los activos
<table><tr><td>Conf</td><td>Integ</td><td>Disp</td></tr><tr><td>2</td><td>3</td><td>3</td></tr></table>Impacto Directo</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td rowspan="2">Dispositivos de comunicaciones
Router
Switch</td><td>Mala gestión de contrase-ñas</td><td>Clave router wireless insegura</td><td rowspan="2">Operacional
Tiempo de reparación; Pérdida de Tiempo Costo financiero de habilidades específicas para reparar el daño o reemplazo; Imagen, reputación y buena voluntad
Valoración:
No tiene precio la reputación y buen nombre; por reemplazo $800</td><td>Bajo</td><td>No</td><td>Inefi-ciente</td><td>…</td><td>Fácil</td><td>Media</td></tr>
<tr><td>Incumpli-miento de disponibi-lidad</td><td>Red administrativa funciona única-mente cuando se encuentra el Propietario.</td><td>Bajo</td><td>No</td><td>Inefi-ciente</td><td>5/7</td><td>Muy fácil</td><td>Alta</td></tr>
</table>

Tabla 6.17: Evaluación de la Probabilidad de incidentes (Fuente: IEC/ITC 27005, 2008, págs. 14,15) (Elaborado por: Investigador) (cont.)

Tabla 6.17: Evaluación de la Probabilidad de incidentes (cont.)

<table>
<tr><th rowspan="2">Activos</th><th colspan="2">Escenario de incidente</th><th rowspan="2">Consecuencia

0 Nada grave
1 Poco grave
2 Grave
3 Muy Grave</th><th colspan="3">Controles existentes y planificados</th><th colspan="3">Probabilidad</th></tr>
<tr><th>Amenaza</th><th>Vulnerabilidad</th><th>Eficacia</th><th>Imple-mentación</th><th>Estado</th><th>Frecuencia de amenaza</th><th>Facilidad con que la vulnerabilidad puede ser explo-tada:Difícil Fácil- Muy Fácil</th><th>Resultado de la Pro-babilidad: Muy baja, Baja Media, Alta,Muy alta</th></tr>
<tr><td>…</td><td>…</td><td>…
Sistema de Gestión de Información</td><td>Pérdida de compromiso de los activos
<table><tr><td>Conf</td><td>Integ</td><td>Disp</td></tr><tr><td>0</td><td>2</td><td>3</td></tr></table>Impacto Indirecto</td><td>…</td><td>…</td><td>…</td><td>…</td><td>…</td><td>…</td></tr>
<tr><td>Interfaz de comunica cio-nes:
Tarjetas de red inalámbricas
Tarjetas de red Ethernet</td><td>Fenómeno climático</td><td>Tormenta eléctrica</td><td>Operacional
Tiempo de reparación
Costo financiero de habilidades específicas para reparar el daño o reemplazo
Valoración:$ 20 cada tarjeta
Pérdida de compromiso de los activos
<table><tr><td>Conf</td><td>Integ</td><td>Disp</td></tr><tr><td>0</td><td>3</td><td>3</td></tr></table>Impacto Indirecto</td><td>Alto</td><td>Si</td><td>Se justi-fica</td><td>1/20</td><td>Difícil</td><td>Baja</td></tr>
</table>

Tabla 6.17: Evaluación de la Probabilidad de incidentes (Fuente: IEC/ITC 27005, 2008, págs. 14,15) (Elaborado por: Investigador) (cont.)

Tabla 6.17: Evaluación de la Probabilidad de incidentes (cont.)

<table>
<tr><th rowspan="2">Activos</th><th colspan="2">Escenario de incidente</th><th rowspan="2">Consecuencia

0 Nada grave
1 Poco grave
2 Grave
3 Muy Grave</th><th colspan="3">Controles existentes y planificados</th><th colspan="3">Probabilidad</th></tr>
<tr><th>Amenaza</th><th>Vulnerabilidad</th><th>Eficacia</th><th>Imple-mentación</th><th>Estado</th><th>Frecuencia de amenaza</th><th>Facilidad con que la vulnerabilidad puede ser explo-tada:Difícil Fácil- Muy Fácil</th><th>Resultado de la Pro-babilidad: Muy baja, Baja Media, Alta,Muy alta</th></tr>
<tr><td>Toma de decisiones Propietario – Director</td><td>Incumpli-miento de disponi-bilidad.</td><td>Oficina donde está el switch y servidor de Aplicaciones pasa cerrada.</td><td>Operacional: Tiempo de reparación; Pérdida de Tiempo
Valoración: No tiene precio
Pérdida de compromiso de los activos<table><tr><td>Conf</td><td>Integ</td><td>Disp</td></tr><tr><td>3</td><td>3</td><td>3</td></tr></table>Impacto: Directo</td><td>Bajo</td><td>Si</td><td>Inefi-ciente</td><td>3/5</td><td>Fácil</td><td>Alta</td></tr>
<tr><td>Estudiantes</td><td>Incumpli-miento de obligacio-nes
.</td><td>Disminución de estudiantes, afecta económica-mente a la Institución</td><td>Operacional
Imagen, reputación y buen nombre
Valoración
No tiene precio
Impacto Directo</td><td>Media</td><td>Si</td><td>Ine-ficiente</td><td>1/12</td><td>Difícil</td><td>Muy Baja</td></tr>
</table>

Tabla 6.17: Evaluación de la Probabilidad de incidentes (Fuente: IEC/ITC 27005, 2008, págs. 14,15) (Elaborado por: Investigador) (cont.)

Tabla 6.17: Evaluación de la Probabilidad de incidentes (cont.)

<table>
<tr><th rowspan="2">Activos</th><th colspan="2">Escenario de incidente</th><th rowspan="2">Consecuencia

0 Nada grave
1 Poco grave
2 Grave
3 Muy Grave</th><th colspan="3">Controles existentes y planificados</th><th colspan="3">Probabilidad</th></tr>
<tr><th>Amenaza</th><th>Vulnerabilidad</th><th>Eficacia</th><th>Implementación</th><th>Estado</th><th>Frecuencia de amenaza</th><th>Facilidad con que la vulnerabilidad puede ser explotada:Difícil Fácil- Muy Fácil</th><th>Resultado de la Probabilidad: Muy baja, Baja Media, Alta,Muy alta</th></tr>
<tr><td>…</td><td>…</td><td>…</td><td>Pérdida de compromiso de los activos<table><tr><td>Conf</td><td>Integ</td><td>Disp</td></tr><tr><td>3</td><td>3</td><td>3</td></tr></table></td><td>…</td><td>…</td><td>…</td><td>…</td><td>…</td><td>…</td></tr>
<tr><td>Laboratorio de Tics</td><td>Pérdida de ventaja competiti-va</td><td>No hay quien haga seguimiento de las incidencias de seguridad informática, lo que podría conllevar la dis-minución de es-tudiantes, por ende disminución de ingresos.</td><td>Operacional
Imagen, reputación y buen nombre
Valoración
$ 8000 si todo el laboratorio se daña</td><td>Bajo</td><td>No</td><td>Inefi-ciente</td><td>20/20</td><td>Muy fácil</td><td>Muy Alta</td></tr>
</table>

Tabla 6.17: Evaluación de la Probabilidad de incidentes (Fuente: IEC/ITC 27005, 2008, págs. 14,15) (Elaborado por: Investigador) (cont.)

Tabla 6.17: Evaluación de la Probabilidad de incidentes (cont.)

<table>
<tr><th rowspan="2">Activos</th><th colspan="2">Escenario de incidente</th><th rowspan="2">Consecuencia

0 Nada grave
1 Poco grave
2 Grave
3 Muy Grave</th><th colspan="3">Controles existentes y planificados</th><th colspan="3">Probabilidad</th></tr>
<tr><th>Amenaza</th><th>Vulnerabilidad</th><th>Eficacia</th><th>Imple-men-tación</th><th>Estado</th><th>Frecuencia de amenaza</th><th>Facilidad con que la vulnerabilidad puede ser explo-tada:Difícil Fácil- Muy Fácil</th><th>Resultado de la Pro-babilidad: Muy baja, Baja Media, Alta,Muy alta</th></tr>
<tr><td>Servicios esenciales Energía eléctrica</td><td>Incumpli-miento de disponi-bilidad.</td><td>Laboratorio Tics, equipos del área administrativa
No tienen un UPS para apagar correctamente los mismos.</td><td>Operacional
Pérdida de Tiempo
Valoración
Pago mensual restado por el cálculo del tiempo de corte
Pérdida de compromiso de los activos<table><tr><td>Conf</td><td>Integ</td><td>Disp</td></tr><tr><td>3</td><td>3</td><td>3</td></tr></table>Impacto Indirecto</td><td>Medio</td><td>Si</td><td>Se justifica</td><td>3/365</td><td>Difícil</td><td>Muy baja</td></tr>
</table>

Tabla 6.17: Evaluación de la Probabilidad de incidentes (Fuente: IEC/ITC 27005, 2008, págs. 14,15) (Elaborado por: Investigador) (cont.)

Tabla 6.17: Evaluación de la Probabilidad de incidentes (cont.)

Activos	**Escenario de incidente**		**Consecuencia** **0 Nada grave** **1 Poco grave** **2 Grave** **3 Muy Grave**	**Controles existentes y planificados**			**Probabilidad**		
	Amenaza	**Vulnerabilidad**		**Eficacia**	**Implementación**	**Estado**	**Frecuencia de amenaza**	**Facilidad con que la vulnerabilidad puede ser explotada:Difícil Fácil- Muy Fácil**	**Resultado de la Probabilidad: Muy baja, Baja Media, Alta,Muy alta**
Comunicación Teléfono Internet	Incumplimiento de disponibilidad.	Falta de seguimiento de incidentes de seguridad informática Los datos del sistema que son publicados en la página web no estarían disponibles.	**Operacional** Pérdida de Tiempo **Valoración** Pago de servicio sin usar $ 256 Pago de servicio Internet sin usar $216 **Pérdida de compromiso de los activos** Conf: 2 | Integ: 2 | Disp: 3 **Impacto** Indirecto	Bajo	No	Ineficiente	14/31 Ver Anexo 11	Muy Fácil	Muy Alta

Tabla 6.17: Evaluación de la Probabilidad de incidentes (Fuente: IEC/ITC 27005, 2008, págs. 14,15) (Elaborado por: Investigador)

Nivel de estimación del riesgo

Tiene como entrada una lista de escenarios de incidente con sus consecuencias relacionadas a los activos y procesos de negocio y su probabilidad (cualitativa o cuantitativa)

"Valuación del riesgo es el proceso general de análisis del riesgo y evaluación del riesgo" (ISO/IEC Guía 73:2002)". (ISO/ICE, ITC, 2005, pág. 11).

Activos y proceso de negocio	**Escenario de incidente**		**Probabilidad**
	Amenaza	**Vulnerabilidad**	1 Muy baja 2 Baja 3 Media 4 Alta 5 Muy alta
Formación de niños, niñas y adolescentes	Acoso intimidación	Control de acceso a Internet	2
	Acoso para gratificación sexual		2
	Han enviado fotos, videos, sonidos de una persona sin su consentimiento		3

Tabla 6.18: Nivel de estimación del Riesgo (Fuente: IEC/ITC 27005, 2008, págs. 16) (Elaborado por: Investigador) (cont.)

Tabla 6.18: Evaluación del Riesgo (cont.)

Activos y proceso de negocio	**Escenario de incidente**		**Probabilidad**
	Amenaza	**Vulnerabilidad**	1 Muy baja 2 Baja 3 Media 4 Alta 5 Muy alta
	Sexting		2
	Utilización de la identidad personal por parte de otra persona		2
Equipos fijos Computadores del Laboratorio Tics	Polvo, corrosión	Falta de aseo en donde están los CPUs puede causar mal funciona- miento en los componentes electrónicos	3
	Daño de periféricos	Utilización poco cuidadosa de los periféricos	4
	Abuso de derechos	Falta de informes de fallos, del Profesor de Tics	3

Tabla 6.18: Nivel de estimación del Riesgo (Fuente: IEC/ITC 27005, 2008, págs. 16)
(Elaborado por: Investigador) (cont.)

Tabla 6.18: Nivel de estimación del Riesgo (cont.)

Activos y proceso de negocio	**Escenario de incidente**		**Probabilidad**
	Amenaza	**Vulnerabilidad**	1 Muy baja 2 Baja 3 Media 4 Alta 5 Muy alta
… Equipos fijos Computadores del Laboratorio Tics	Incendio	Cables en el piso, los estudiantes les pisan al sentarse o cambiar se de sitio	4
	Sobrecarga eléctrica	Cables eléctricos y cortapicos conectados uno a continuación de otro para abastecer las tomas eléctricas de los 15 computadores	4
Servidor de control de acceso a Internet	Abuso de derechos	Eliminación del log al reiniciar el computador por el Deep Freeze instalado. No respaldar el log	5

Tabla 6.18: Nivel de estimación del Riesgo (Fuente: IEC/ITC 27005, 2008, págs. 16) (Elaborado por: Investigador) (cont.)

Tabla 6.18: Nivel de estimación del Riesgo (cont.)

Activos y proceso de negocio	**Escenario de incidente**		**Probabilidad**
	Amenaza	**Vulnerabilidad**	1 Muy baja 2 Baja 3 Media 4 Alta 5 Muy alta
Sistema Operativo y Microsoft Office	Copia de software fraudulento	Licencias de uso, y por ende el software pirata es vulnerable a instalación de código malicioso, virus, entre otros	1
Servicio de mantenimiento o administración del software	Virus, código malicioso	Cortes de Internet frecuentes Deep Freeze al reiniciar el computador regresa al estado inicial pero la partición D del disco si permite guardar información	5

Tabla 6.18: Evaluación del Riesgo (Fuente: IEC/ITC 27005, 2008, págs. 14,15) (Elaborado por: Investigador) (cont.)

Tabla 6.18: Evaluación del Riesgo (cont.)

Activos y proceso de negocio	**Escenario de incidente**		**Probabilidad**
	Amenaza	**Vulnerabilidad**	1 Muy baja 2 Baja 3 Media 4 Alta 5 Muy alta
Deep Freeze	Mal funcionamiento del software	No entrega la clave al profesor de Tics por ende no se actualiza antivirus ni software	5
Antivirus	Incumplimiento en el mantenimiento del software del antivirus	Antivirus caducado y también no se actualiza la base de datos de virus por el Deep freeze instalado.	4
Navegadores para Internet	Código malicioso	Software de navegadores se actualiza y se elimina la actualización al reiniciar el equipo por el deep Freeze.	5

Tabla 6.18: Evaluación del Riesgo (Fuente: IEC/ITC 27005, 2008, págs. 16) (Elaborado por: Investigador) (cont.)

Tabla 6.18: Nivel de estimación del Riesgo (cont.)

Activos y proceso de negocio	**Escenario de incidente**		**Probabilidad**
	Amenaza	**Vulnerabilidad**	1 Muy baja 2 Baja 3 Media 4 Alta 5 Muy alta
Red Ethernet, Red inalámbrica 802.11 a/b/c/n/g	Incumplimiento de disponibilidad Conflictos IP Arquitectura de red inadecuada	Switch ubicado en un área donde no se prende si no llega el propietario. Inadecuada administración de la red. Direccionamiento IP de los equipos del área administrativa sin orden. Tienen 2 redes planas separadas, lo que a la larga impedirá el crecimiento tecnológico.	4
Dispositivos de comunicaciones Router Switch	Mala gestión de contraseñas	Clave router wireless insegura	3

Tabla 6.18: Nivel de estimación del riesgo y evaluación del riesgo (Fuente: IEC/ITC 27005, 2008, págs. 16) (Elaborado por: Investigador) (cont.)

Tabla 6.18: Nivel de estimación del riesgo y evaluación del riesgo (cont.)

Activos y proceso de negocio	**Escenario de incidente**		**Probabilidad**
	Amenaza	**Vulnerabilidad**	1 Muy baja 2 Baja 3 Media 4 Alta 5 Muy alta
… Dispositivos de comunicaciones Router Switch	Incumplimiento de disponibilidad	Red administrativa funciona únicamente cuando se encuentra el Propietario. Sistema de Gestión de Información	4
Interfaz de comunicaciones: Tarjetas de red inalámbricas y Ethernet	Fenómeno climático	Tormenta eléctrica	2
Toma de decisiones Pro-pietario Director	Incumplimiento de disponibilidad.	Oficina donde está el switch y servidor de Aplicaciones pasa cerrada.	4

Tabla 6.18: Nivel de estimación del Riesgo (Fuente: IEC/ITC 27005, 2008, págs. 16) (Elaborado por: Investigador) (cont.)

Tabla 6.18: Nivel de estimación del riesgo (cont.)

Activos y proceso de negocio	**Escenario de incidente**		**Probabilidad**
	Amenaza	**Vulnerabilidad**	1 Muy baja 2 Baja 3 Media 4 Alta 5 Muy alta
Estudiantes	Incumplimiento de obligaciones	Disminución de estudiantes, afecta económica-mente a la Institución	5
Laboratorio de Tics	Pérdida de ventaja competitiva	No hay quien haga seguimiento de las incidencias de seguridad informática, lo que podría conllevar la disminución de estudiantes, por ende disminución de ingresos.	5
Servicios esenciales Energía eléctrica	Incumplimiento de disponibilidad.	Laboratorio TICs. Equipos del área administrativa No tienen un UPS para apagar correctamente los mismos.	1

Tabla 6.18: Nivel de estimación del Riesgo (Fuente: IEC/ITC 27005, 2008, págs. 16)
(Elaborado por: Investigador) (cont.)

Tabla 6.18: Nivel de estimación del Riesgo (cont.)

Activos y proceso de negocio	**Escenario de incidente**		**Probabilidad**
	Amenaza	**Vulnerabilidad**	1 Muy baja 2 Baja 3 Media 4 Alta 5 Muy alta
Comunica-ción Teléfono Internet	Incumplimien to de dis-ponibilidad.	Falta de seguimiento de incidentes de seguridad informática Los datos del sistema que son publicados en la página web no estarían disponibles.	5

Tabla 6.18: Nivel de estimación del Riesgo (Fuente: IEC/ITC 27005, 2008, págs. 16)
(Elaborado por: Investigador)

6.8.2.6.12 Evaluación del riesgo

"Evaluación del riesgo es proceso de comparar el riesgo estimado con el criterio de riesgo dado para determinar la importancia del riesgo. (ISO/IEC Guía 73:2002)" (ISO/ICE, ITC, 2005, pág. 11).

Activos y proceso de negocio	**Escenario de incidente**		**Impacto de la amenaza**	**Probabilidad**	**Medición del riesgo**	**Priorización**
	Amenaza	**Vulnerabilidad**	1 Muy baja 2 Baja 3 Media 4 Alta 5 Muy alta	1 Muy baja 2 Baja 3 Media 4 Alta 5 Muy alta		
Formación de niños, niñas y adolescentes	Acoso intimidación	Control de acceso a Internet	5	2	10	19
	Acoso para gratificación sexual		5	2	10	16
	Han enviado fotos, videos, sonidos de una persona sin su consentimiento		5	3	15	11
	Sexting		5	2	10	17
	Utilización de la identidad personal por parte de otra persona		5	2	10	18

Tabla 6.19: Evaluación del Riesgo (Fuente: IEC/ITC 27005, 2008, págs. 16) (Elaborado por: Investigador) (cont.)

Tabla 6.19: Evaluación del Riesgo (cont.)

Activos y proceso de negocio	**Escenario de incidente**		**Impacto de la amenaza**	**Probabilidad**	**Medición del riesgo**	**Priorización**
	Amenaza	**Vulnerabilidad**	1 Muy baja 2 Baja 3 Media 4 Alta 5 Muy alta	1 Muy baja 2 Baja 3 Media 4 Alta 5 Muy alta		
Equipos fijos Computadores del Laboratorio Tics	Polvo, corrosión	Falta de aseo en donde están los CPUs puede causar mal funciona- miento en los componentes electrónicos	1	3	3	24
	Daño de periféricos	Utilización poco cuidadosa de los periféricos	3	4	12	14
	Abuso de derechos	Falta de informes de fallos, del Profesor de Tics	2	3	6	21

Tabla 6.19: Evaluación del Riesgo (Fuente: IEC/ITC 27005, 2008, págs. 16) (Elaborado por: Investigador) (cont.)

Tabla 6.19: Evaluación del Riesgo (cont.)

Activos y proceso de negocio	**Escenario de incidente**		**Impacto de la amenaza**	**Probabilidad**	**Medición del riesgo**	**Priorización**
	Amenaza	**Vulnerabilidad**	1 Muy baja 2 Baja 3 Media 4 Alta 5 Muy alta	1 Muy baja 2 Baja 3 Media 4 Alta 5 Muy alta		
… Equipos fijos Computadores del Laboratorio Tics	Incendio	Cables en el piso, los estudiantes les pisan al sentarse o cambiar se de sitio	5	4	20	6
	Sobrecarga eléctrica	Cables eléctricos y cortapicos conectados uno a continuación de otro para abastecer las tomas eléctricas de los 15 computadores	4	4	16	10
Servidor de control de acceso a Internet	Abuso de derechos	Eliminación del log al reiniciar el computador por el Deep Freeze instalado. No respaldar el log	4	5	20	4

Tabla 6.19: Evaluación del Riesgo (Fuente: IEC/ITC 27005, 2008, págs. 16) (Elaborado por: Investigador) (cont.)

Tabla 6.19: Evaluación del Riesgo (cont.)

Activos y proceso de negocio	Escenario de incidente		Impacto de la amenaza	Probabilidad	Medición del riesgo	Priorización
	Amenaza	Vulnerabilidad	1 Muy baja 2 Baja 3 Media 4 Alta 5 Muy alta	1 Muy baja 2 Baja 3 Media 4 Alta 5 Muy alta		
Sistema Operativo y Microsoft Office	Copia de software fraudulento	Licencias de uso, y por ende el software pirata es vulnerable a instalación de código malicioso, virus, entre otros	5	1	5	22
Servicio de mantenimiento o administración del software	Virus, código malicioso	Cortes de Internet frecuentes Deep Freeze al reiniciar el computador regresa al estado inicial pero la partición D del disco si permite guardar información	3	5	15	12

Tabla 6.19: Evaluación del Riesgo (Fuente: IEC/ITC 27005, 2008, págs. 14,15) (Elaborado por: Investigador) (cont.)

Tabla 6.19: Evaluación del Riesgo (cont.)

Activos y proceso de negocio	Escenario de incidente		Impacto de la amenaza	Probabilidad	Medición del riesgo	Priorización
	Amenaza	Vulnerabilidad	1 Muy baja 2 Baja 3 Media 4 Alta 5 Muy alta	1 Muy baja 2 Baja 3 Media 4 Alta 5 Muy alta		
Deep Freeze	Mal funcionamiento del software	No entrega la clave al profesor de Tics por ende no se actualiza antivirus ni software	2	5	10	15
Antivirus	Incumplimiento en el mantenimiento del software del antivirus	Antivirus caducado y también no se actualiza la base de datos de virus por el Deep freeze instalado.	5	4	20	5
Navegadores para Internet	Código malicioso	Software de navegadores se actualiza y se elimina la actualización al reiniciar el equipo por el deep Freeze.	5	5	25	9

Tabla 6.19: Evaluación del Riesgo (Fuente: IEC/ITC 27005, 2008, págs. 16) (Elaborado por: Investigador) (cont.)

Tabla 6.19: Evaluación del Riesgo (cont.)

Activos y proceso de negocio	**Escenario de incidente**		**Impacto de la amenaza**	**Probabilidad**	**Medición del riesgo**	**Priorización**
	Amenaza	**Vulnerabilidad**	1 Muy baja 2 Baja 3 Media 4 Alta 5 Muy alta	1 Muy baja 2 Baja 3 Media 4 Alta 5 Muy alta		
Red Ethernet, Red inalámbrica 802.11 a/b/c/n/g	Incumplimiento de disponibilidad Conflictos IP Arquitectura de red inadecuada	Switch ubicado en un área donde no se prende si no llega el propietario. Inadecuada administración de la red. Direccionamiento IP de los equipos del área administrativa sin orden. Tienen 2 redes planas separadas, lo que a la larga impedirá el crecimiento tecnológico.	5	4	20	2

Tabla 6.19: Evaluación del riesgo (Fuente: IEC/ITC 27005, 2008, págs. 16) (Elaborado por: Investigador) (cont.)

Tabla 6.19: Evaluación del riesgo (cont.)

Activos y proceso de negocio	**Escenario de incidente**		**Impacto de la amenaza**	**Probabilidad**	**Medición del riesgo**	**Priorización**
	Amenaza	**Vulnerabilidad**	1 Muy baja 2 Baja 3 Media 4 Alta 5 Muy alta	1 Muy baja 2 Baja 3 Media 4 Alta 5 Muy alta		
Dispositivos de comunicaciones Router Switch	Mala gestión de contraseñas	Clave router wireless insegura	4	3	12	12
	Incumplimiento de disponibilidad	Red administrativa funciona únicamente cuando se encuentra el Propietario. Sistema de Gestión de Información	5	4	20	7
Interfaz de comunicaciones: Tarjetas de red inalámbricas y Ethernet	Fenómeno climático	Tormenta eléctrica	3	2	6	20

Tabla 6.19: Evaluación del Riesgo (Fuente: IEC/ITC 27005, 2008, págs. 16) (Elaborado por: Investigador) (cont.)

Tabla 6.19: Evaluación del riesgo (cont.)

Activos y proceso de negocio	**Escenario de incidente**		**Impacto de la amenaza**	**Probabilidad**	**Medición del riesgo**	**Priorización**
	Amenaza	**Vulnerabilidad**	1 Muy baja 2 Baja 3 Media 4 Alta 5 Muy alta	1 Muy baja 2 Baja 3 Media 4 Alta 5 Muy alta		
Toma de decisiones Pro-pietario Director	Incumplimiento de disponibilidad.	Oficina donde está el switch y servidor de Aplicaciones pasa cerrada.	5	4	20	8
Estudiantes	Incumplimiento de obligaciones	Disminución de estudiantes, afecta económica-mente a la Institución	1	5	5	23
Laboratorio de Tics	Pérdida de ventaja competitiva	No hay quien haga seguimiento de las incidencias de seguridad informática, lo que podría conllevar la disminución de estudiantes, por ende disminución de ingresos.	5	5	25	1

Tabla 6.19: Evaluación del Riesgo (Fuente: IEC/ITC 27005, 2008, págs. 16) (Elaborado por: Investigador) (cont.)

Tabla 6.19: Evaluación del Riesgo (cont.)

Activos y proceso de negocio	**Escenario de incidente**		**Impacto de la amenaza**	**Probabilidad**	**Medición del riesgo**	**Priorización**
	Amenaza	**Vulnerabilidad**	1 Muy baja 2 Baja 3 Media 4 Alta 5 Muy alta	1 Muy baja 2 Baja 3 Media 4 Alta 5 Muy alta		
Servicios esenciales Energía eléctrica	Incumplimiento de disponibilidad.	Laboratorio TICs. Equipos del área administrativa No tienen un UPS para apagar correctamente los mismos.	2	1	2	25
Comunicación Teléfono Internet	Incumplimiento de disponibilidad.	Falta de seguimiento de incidentes de seguridad informática Los datos del sistema que son publicados en la página web no estarían disponibles.	4	5	20	3

Tabla 6.19: Evaluación del Riesgo (Fuente: IEC/ITC 27005, 2008, págs. 16) (Elaborado por: Investigador)

6.8.2.6.13 Tratamiento de riesgo

"Tratamiento del riesgo es el proceso de tratamiento de la selección e implementación de medidas para modificar el riesgo (ISO/IEC Guía 73:2002)" (ISO/ICE 27001, 2005, pág. 11).

El tratamiento del riesgo se lo realiza con el propietario de la Institución, Profesor de Tics bajo lo dispuesto en la norma ISO 27005 se tiene: aceptar, reducir, retener, transferir.

"Aceptación de riesgo es la decisión de aceptar el riesgo (ISO/IEC Guía 73:2002)" (ISO/ICE, ITC, 2005, pág. 11) .

"Reducción del riesgo son las acciones tomadas para reducir la probabilidad de los riesgos asociados con las consecuencias negativas (ISO/IEC Guía 73:2002)" (IEC/ITC 27005, 2008, pág. 2).

"Retener el riesgo es aceptar el peso de perder o beneficiarse de la ganancia de un riesgo particular (ISO/IEC Guía 73:2002)". (IEC/ITC 27005, 2008, pág. 2).

"Transferir el riesgo es compatir con otra parte el peso de perder o beneficiarse de la ganancia de un riesgo" (IEC/ITC 27005, 2008, pág. 2).

A continuación se presenta la tabla en la que se toma la decisión del tratamiento de riesgo.

Tratamiento de riesgo

Activos y proceso de negocio	Escenario de incidente		Medición del riesgo	Priori-zación	Trata-miento del riesgo
	Amenaza	Vulnerabilidad			
Laboratorio de Tics	Pérdida de ventaja competitiva	No hay quien haga seguimiento de las incidencias de seguridad informática, lo que podría conllevar la disminución de estudiantes, por ende disminución de ingresos.	25	1	Evitar
Red Ethernet, Red inalámbrica 802.11 a/b/c/n/g	Incumplimiento de disponibilidad Conflictos IP Arquitectura de red inadecuada	Switch ubicado en un área donde no se prende si no llega el propietario. Inadecuada administración de la red Direcciona-miento IP de los equipos del área administrativa sin orden. Tienen 2 redes planas separadas, lo que a la larga impedirá el crecimiento tecnológico.	20	2	Evitar

Tabla 6.20: Tabla de Tratamiento de riesgo (IEC/ITC 27005, 2008, pág. 17). (Elaborado por: Investigador) (cont.)

Tabla 6.20: Tabla de Tratamiento de riesgo (cont.)

Activos y proceso de negocio	Escenario de incidente		Medición del riesgo	Priori-zación	Trata-miento del riesgo
	Amenaza	Vulnerabilidad			
Comunica-ción Teléfono Internet	Incumplimiento de disponibilidad	Falta de seguimiento de incidentes de seguridad informática Los datos del sistema que son publicados en la página web no estarían disponibles.	20	3	Reducir
Servidor de control de acceso a Internet	Abuso de derechos	Eliminación del log al reiniciar el computador por el Deep Freeze instalado. No respaldar el log	20	4	Reducir
Antivirus	Incumplimiento en el mantenimiento del software del antivirus	Antivirus caducado y también no se actualiza la base de datos de virus por el Deep freeze instalado.	20	5	Evitar
Equipos del Laboratorio TicsICs	Incendio	Cables en el piso, los estudiantes les pisan al sentarse o cambiar se de sitio	20	6	Reducir

Tabla 6.20: Tabla de Tratamiento de riesgo (IEC/ITC 27005, 2008, pág. 17). (Elaborado por: Investigador) (cont.)

Tabla 6.20: Tabla de Tratamiento de riesgo (cont.)

Activos y proceso de negocio	Escenario de incidente		Medición del riesgo	Priori-zación	Trata-miento del riesgo
	Amenaza	Vulnerabilidad			
Switch	Incumplimiento de disponibilidad	Red administrativa funciona únicamente cuando se encuentra el Propietario. Sistema de Gestión de Información	20	7	Evitar
Toma de decisiones Propietario – Director	Incumplimiento de disponibilidad.	Oficina donde está el switch y servidor de Aplicaciones pasa cerrada.	20	8	Retener
Navegadores para Internet	Código malicioso	Software de navegadores se actualiza y se elimina la actualización al reiniciar el equipo por el deep Freeze.	25	9	Evitar
Computadores Laboratorio TICs	Sobrecarga eléctrica	Cables eléctricos y cortapicos conectados uno a continuación de otro para abastecer las tomas eléctricas de los 15 computadores	16	10	Reducir

Tabla 6.20: Tabla de Tratamiento de riesgo (IEC/ITC 27005, 2008, pág. 17). (Elaborado por: Investigador) (cont.)

Tabla 6.20: Tabla de Tratamiento de riesgo (cont.)

Activos y proceso de negocio	Escenario de incidente		Medición del riesgo	Priori-zación	Trata-miento del riesgo
	Amenaza	Vulnerabilidad			
Formación de niños, niñas y adolescentes	Envío fotos, videos, sonidos de una persona sin su consentimiento	Control de acceso a Internet	15	11	Evitar
Servicio de manteni-miento o administración del software	Virus, código malicioso	Cortes de Internet frecuentes Deep Freeze al reiniciar el computador regresa al estado inicial pero la partición D del disco si permite guardar información	15	12	Reducir
Router	Mala gestión de contraseñas	Clave router wireless insegura	12	13	Eliminar
Computadores del Laboratorio de Tics	Daño de periféricos	Utilización poco cuidadosa de los periféricos	12	14	Transferir
Deep Freeze	Mal funciona -miento del software	No entrega la clave al profesor de TICs por ende no se actualiza antivirus ni software	10	15	Reducir

Tabla 6.20: Tabla de Tratamiento de riesgo (IEC/ITC 27005, 2008, pág. 17). (Elaborado por: Investigador) (cont.)

Tabla 6.20: Tabla de Tratamiento de riesgo (cont.)

Activos y proceso de negocio	Escenario de incidente		Medición del riesgo	Priori-zación	Trata-miento del riesgo
	Amenaza	Vulnerabilidad			
Formación de niños, niñas y adolescentes	Acoso para gratificación sexual	Control de acceso a Internet	10	16	Reducir
	Sexting	Control de acceso a Internet	10	17	Reducir
	Utilización de la identidad personal por parte de otra persona	Control de acceso a Internet	10	18	Reducir
	Acoso intimidación	Control de acceso a Internet	10	19	Reducir
Interfaz de comunica - ciones: • Tarjetas de red inalámbricas y ethernet	Fenómeno climático	Tormenta eléctrica	6	20	Reducir

Tabla 6.20: Tabla de Tratamiento de riesgo (IEC/ITC 27005, 2008, pág. 17). (Elaborado por: Investigador) (cont.)

Tabla 6.20: Tratamiento de riesgo (cont.)

Activos y proceso de negocio	Escenario de incidente		Medición del riesgo	Priori-zación	Trata-miento del riesgo
	Amenaza	Vulnerabilidad			
Computado-res del Laboratorio TICs	Abuso de derechos	Falta de informes de fallos, del Profesor de TICs	6	21	Reducir
Sistema Operativo y Microsoft Office	Copia de software fraudulento	Licencias de uso, y por ende el software pirata es vulnerable a instalación de código malicioso, virus, entre otros	5	22	Retener
Equipos fijos	Polvo, corrosión	Falta de aseo en donde están los CPUs puede causar mal funciona- miento en los componentes electrónicos	3	23	Reducir
Servicios esenciales Energía eléctrica	Incumplimiento de disponibilidad.	Laboratorio TICs. Equipos del área administrativa No tienen un UPS para apagar correctamente los mismos.	2	24	Retener

Tabla 6.20: Tabla de Tratamiento de riesgo (IEC/ITC 27005, 2008, pág. 17). (Elaborado por: Investigador)

6.8.2.6.14 Enunciado de aplicabilidad

"Enunciado de aplicabilidad es un enunciado documentado que describe los objetivos de control y controles que son relevantes y aplicables al SGSI de la organización" (ISO/IEC Guía 73:2002)" (ISO/ICE, ITC, 2005, pág. 12).

Objetivos de Control	Controles	Aplicabilidad		Justificación
		Si	No	
Política de seguridad informática	Documento de política de seguridad informática	X		Es necesario establecer políticas ya que no existen y posterior a ello hacer un seguimiento de las mismas
	Revisión de la política de seguridad informática		X	
Organización interna	Compromiso con los propietarios con la seguridad informática	X		Es importante tener una correcta organización interna para poder realizar un seguimiento y monitoreo adecuado de la seguridad informática
	Coordinación de la seguridad informática	X		
	Asignación de responsabilidades de la seguridad informática	X		
	Proceso de autorización para los medios de procesamiento de información	X		
	Acuerdos de confidencialidad	X		
	Contacto con autoridades	X		

Tabla 6.21: Enunciado de aplicabilidad (Fuente: IEC/ITC ISO 27001, 2005) (Elaborado por: Investigador) (cont.)

Tabla 6.21: Enunciado de aplicabilidad (cont.)

Objetivos de Control	Controles	Aplicabilidad		Justificación
		Si	No	
…	Contacto con grupos de interés especial	X		…
Organización interna	Revisión independiente de la seguridad informática	X		
	Documento de políticas de Seguridad Informática	X		
Entidades externas	Identificación de riesgos relacionados con entidades externas	X		Es importante realizar estos controles para garantizar que la seguridad informática será integral
	Tratamiento de la seguridad cuando se trabaja con estudiantes.	X		
Responsabilidad por los activos	Inventario de activos	X		Los activos tecnológicos son valiosos y representan una inversión para la Institución
	Propiedad de los activos	X		
	Uso aceptable de los activos	X		
Clasificación de la información	Lineamientos de clasificación	X		La información debe estar clasificada y en orden
	Etiquetado y manejo de la información	X		
Seguridad de los Recursos Humanos antes del empleo	Roles y responsabilidades	X		El elemento humano puede ser el más peligroso por ello es necesario que recursos
	Selección	X		
	Términos y condiciones de empleo	X		

Tabla 6.21: Enunciado de aplicabilidad (Fuente: IEC/ITC ISO 27001, 2005) (Elaborado por: Investigador) (cont.)

Tabla 6.21: Enunciado de aplicabilidad (cont.)

Objetivos de Control	**Controles**	**Aplicabilidad**		**Justificación**
		Si	No	
Seguridad de los Recursos Humanos durante el empleo	Gestión de responsabilidades	X		… humanos tome en cuenta la seguridad informática
	Capacitación y educación en seguridad de la información	X		
	Proceso disciplinario	X		
Seguridad de los Recursos Humanos en terminación o cambio de empleo	Responsabilidades en terminación	X		
	Devolución de activos	X		
	Eliminación de derechos de acceso	X		
Áreas seguras	Perímetro de seguridad física	X		La inversión de los activos del Centro Educativo La Pradera merece estar en áreas protegidas
	Controles de entrada físicos	X		
	Seguridad de oficinas, aulas y medios	X		
	Protección contra amenazas externas y ambientales	X		
	Trabajo en áreas seguras	X		

Tabla 6.21: Enunciado de aplicabilidad (Fuente: IEC/ITC ISO 27001, 2005) (Elaborado por: Investigador) (cont.)

Tabla 6.21: Enunciado de aplicabilidad (cont.)

Objetivos de Control	**Controles**	Aplicabilidad		**Justificación**
		Si	No	
Seguridad del equipo	Ubicación y protección del equipo	X		Es importante para la seguridad informática tener protegidos sus activos tecnológicos
	Servicios públicos	X		
	Seguridad en el cableado	X		
	Mantenimiento de equipo			
	Seguridad del equipo fuera del CELP	X		Es necesario garantizar la seguridad informática de los activos fuera del mismo.
Gestión de la seguridad en redes	Controles de red	X		La red es muy importante ya que permite compartir, intercambiar, modificar información, acceder al sistema
	Seguridad de los servicios de red	X		
Gestión de medios	Gestión de los servicios removibles	X		Es importante ya que ayuda a prevenir, evitar la divulgación, modificación, eliminación o destrucción no autorizada de los activos, interrupción de actividades
	Eliminación de los medios	X		
	Procedimientos de manejo de información	X		
	Seguridad de documentación del sistema	X		

Tabla 6.21: Enunciado de aplicabilidad (Fuente: IEC/ITC ISO 27001, 2005) (Elaborado por: Investigador) (cont.)

Tabla 6.21: Enunciado de aplicabilidad (cont.)

Objetivos de Control	Controles	Aplicabilidad		Justificación
		Si	No	
Monitoreo	Registro de auditoría	X		Es importante ya que permite detectar actividades de procesamiento de información no autorizadas
	Uso del sistema de monitoreo	X		
	Protección de la información del registro	X		
	Registros del administrador y operador	X		
	Registro de fallas	X		
Control de acceso	Política de Control de acceso	X		Es importarte controlar el acceso a la información
Gestión del acceso del usuario de sistemas de información	Inscripción del usuario		X	Es importante asegurar el acceso del usuario autorizado y evitar el acceso no autorizado a los sistemas de información, para este Plan SGSI no está considerado el área del Sistema de Gestión de información
	Gestión de privilegios		X	
	Gestión de la clave de usuario		X	
	Revisión de los derechos de acceso del usuario		X	
Responsabilidades del usuario	Uso de clave	X		Es importante porque permite evitar el acceso de usuarios no autorizados, y el compromiso o robo de la información y los medios de procesamiento de la misma.
	Equipo de usuario desatendido	X		
	Política de pantalla y escritorio limpio		X	

Tabla 6.21: Enunciado de aplicabilidad (Fuente: IEC/ITC ISO 27001, 2005) (Elaborado por: Investigador) (cont.)

Tabla 6.21: Enunciado de aplicabilidad (cont.)

Objetivos de Control	Controles	Aplicabilidad		Justificación
		Si	No	
				No es necesario la política de escritorio limpio ya que se utiliza el Deep freeze.
Control de acceso a redes	Política sobre el uso de servicios de red	X		Es importante ya que se puede evitar el acceso no-autorizado a los servicios en red
	Autenticación del usuario para conexiones externas	X		
	Identificación del equipo en red	X		
	Segregación de redes	X		
	Protección del puerto de diagnóstico remoto	X		
	Control de 'routing' de redes	X		
Gestión de incidentes de seguridad de información	Reporte de eventos de seguridad de información	X		La información de los eventos y debilidades en la seguridad de la información asociados con los sistemas de información sea comunicada de una manera que permita tomar acción correctiva oportuna.
	Reporte de debilidades de seguridad de la información	X		

Tabla 6.21: Enunciado de aplicabilidad (Fuente: IEC/ITC ISO 27001, 2005) (Elaborado por: Investigador)

Luego de definir los objetivos de control se establecen los siguientes documentos:

- Instructivo para etiquetado y manejo de información
- Políticas de seguridad informática
- Documento de acuerdo de confidencialidad
- Lineamientos de uso aceptable de los activos informáticos
- Instructivo para nombrar respaldos
- Instructivo para inventario de activos
- Formato para solicitar salida de equipos fuera de la Institución
- Formato para la devolución de equipos
- Formato de solicitud de acceso a sitios web
- Formato de Equipo de usuario desatendido que requiere reparación
- Registro de compromiso de los Propietarios y Dirección
- Reporte de incidentes de seguridad informática
- Registro de incidencias a los proveedores de Telecomunicaciones
- Instructivo para revisión de políticas de seguridad informática
- Instructivo para control de routing de redes
- Instructivo para segregación de redes
- Documento de entrega de respaldos a los propietarios
- Reporte de incidencias de seguridad informática a los propietarios
- Registro de contacto con las autoridades
- Formato de uso de activos tecnológicos

Instructivo para etiquetado y manejo de la Información

Instructivo para etiquetado y manejo de la Información			
Fecha de emisión:	**Fecha de modificación**	**Fecha de aprobación**	**Identificador I-SEC-01**
Elaborado por:		**Revisado y aprobado por:**	

I. INTRODUCCIÓN

Este documento describe la metodología a utilizar para la asignación de códigos para los activos, la cual se aplicará en el Centro Educativo La Pradera para identificar los documentos del Plan de Seguridad Informática.

II. PROCEDIMIENTO PARA ETIQUETAR

Todos los documentos emitidos en el Plan de seguridad informática serán identificados con un identificador del documento que constituye una numeración alfanumérica única para cada documento; las funciones para el documento pueden ser:

Inicial	Función	Descripción
I	Instructivo	Es un documento en donde se define paso a paso cómo se debe realizar una determinada actividad.
F	Formulario	Es un documento utilizado para registrar los resultados de una actividad.
M	Manual	Es un documento que contiene información del Plan se Seguridad Informática.
P	Procedimientos	Es un documento que describe la forma para llevar a cabo una actividad o proceso.

Documento 2: Instructivo para etiquetado y manejo de la información (cont.)

Documento 2: Instructivo para etiquetado y manejo de la información (cont.)

Instructivo para etiquetado y manejo de la Información

Inicial	Función	Descripción
R	Registros	Son documentos que permiten evidenciar ciertas actividades para demostrar a terceros que un requisito del Plan de Seguridad informática se está cumpliendo.
L	Políticas	Es un documento que sirve de lineamiento o guía que se debe cumplir en el Centro Educativo La Pradera.
T	Tablas	Es un documento del Plan de Seguridad informática el cual contiene información relevante de la organización.
G	Guía	Es un documento que sirve como orientación o consulta y permite localizar fácilmente, en un documento gran parte de los documentos relacionadas con un aspecto.
D	Documento	Es un documento de compromiso

Los dos siguientes caracteres identifican a cual área de la empresa pertenece el documento según la siguiente lista:

Iniciales	Área
SEC	Secretaría
INS	Inspección
LAB	Laboratorio TICs
DIR	Dirección
PRO	Propietarios
SOF	Software
TEC	Encargado de Tecnología
COR	Coordinador de la Seguridad Informática
DOC	Personal Docente
ADM	Personal Administrativo

Documento 2: Instructivo para etiquetado y manejo de la información (cont.)

Documento 2: Instructivo para etiquetado y manejo de la información (cont.)

Instructivo para etiquetado y manejo de la Información

Los tres siguientes dígitos muestran el orden secuencial del documento. El siguiente carácter, que es alfanumérico representa la modificación del documento, al final se debe incluir un anexo, donde se enumeren las razones por la cuales se ha modificado dicho documento.

En el anexo mencionado, se especificará el (los) tipo(s) de cambio(s) aplicado(s) al documento de la siguiente forma:

Inicial	Nombre	Descripción
A	Añadido	Se usará para añadir un párrafo o línea o renglón al documento
F	Fusionado	Es para cuando se unifican dos o más documentos en uno solo
M	Modificado	Se usará cuando el cambio únicamente se realiza en algunas partes del documento
R	Reemplazado	Se usará cuando el documento es cambiado totalmente

Documento 2: Instructivo para etiquetado y manejo de la información

Fuente: (Chamorro, V., 2013, págs. 113-115) (Elaborado por: Investigador)

Políticas de Seguridad Informática

Documento de Políticas de Seguridad Informática			
Fecha de Emisión:	**Fecha Modificación:**	**Fecha de Aprobación:**	**Identificador** L-COR-01
Elaborado por:		**Revisado y Aprobado por:**	

I. INTRODUCCIÓN

El documento de políticas presenta las políticas de Seguridad Informática que serán aplicadas en el Centro Educativo La Pradera.

II. POLÍTICAS

Las políticas que se aplican en el Centro Educativo la Pradera involucran a: propietarios, dirección, personal administrativo, personal docente, encargado de tecnología (en el caso de no existir asumirá el rol el profesor de Tics) padres de familia, estudiantes.

Propietarios – Dirección debe:

1. Aprobar un documento de políticas, el mismo que será publicado y comunicado a todo el personal docente, administrativo, estudiantes, padres de familia y entidades externas relevantes.
2. Establecer un documento con las políticas de seguridad informática para ser aplicadas en el Centro Educativo La Pradera.

Documento 3: Políticas de seguridad informática (cont.)

Documento 3: Políticas de Seguridad Informática (cont.)

Documento de Políticas de Seguridad Informática
3. Apoyar activamente la seguridad dentro del Centro Educativo a través de un compromiso demostrado y reconocimiento de las responsabilidades de la seguridad de la información. 4. Coordinar las actividades de seguridad de la información junto con los representantes de las diferentes áreas: administrativos, docentes, profesor de Tics (en caso de no existir un encargado de Tecnología para la Institución), estudiantes, padres de familia. 5. Designar a la persona encargada de coordinar las actividades de seguridad informática. 6. Definir claramente las responsabilidades de la seguridad de información. 7. Realizar una auditoría interna por lo menos una vez al año para verificar el estado del Plan de Seguridad informática, deberá ser realizada por una persona externa a la institución y deberá ser documentada y registrada. 8. Tratar todos los requerimientos de seguridad identificados antes de otorgar a los padres de familia, o nuevos clientes acceso a la información o activos de la organización. 9. Requerir que los docentes, padres de familia, estudiantes, personal administrativo o terceros, apliquen la seguridad en concordancia con las políticas y procedimientos establecidos de la organización. 10. Establecer en contratos con terceras personas los acuerdos necesarios que involucren acceso, procesamiento, comunicación o manejo a la información o los medios de procesamiento de la misma, debe abarcar los requerimientos de seguridad necesaria.

Documento 3: Políticas de seguridad informática (cont.)

Documento 3: Políticas de Seguridad Informática (cont.)

Documento de Políticas de Seguridad Informática
11. Entregar la clave del Deep Freeze al encargado de Tecnología (en caso de no existir, el profesor de Tics asumirá esta función) con la finalidad de que mantenga actualizado el antivirus y software, la misma que deberá ser cuidada y no podrá ser divulgada a nadie. 12. Cambiar la clave del Deep Freeze cuando haya cambio del personal de Tecnología o profesor de Tics. 13. Contactar con el técnico de sistemas para arreglos de equipos tecnológicos apenas sucede el incidente previo informe del coordinador de seguridad, o cada semestre para el mantenimiento respectivo para proveer su continua disponibilidad e integridad. 14. Proveer de insumos de oficina para impresoras: cartuchos, tinta, tóneres, cintas para el área administrativa y sala de docentes periódicamente; carpetas archivadoras para el coordinador de seguridad de la información; dvds para respaldo diario de la base de datos para el encargado de tecnología (de no existir asumirá el rol el profesor de Tic), dvds y disco duro externo para respaldos históricos de secretaría, dvds para respaldo de información de inspección, DOBE, Coordinación Académica. 15. Proteger las áreas que contienen información y medios de procesamiento de información utilizando perímetros de seguridad (barreras tales como paredes) y puertas de ingreso controlado o recepcionistas).

Documento 3: Políticas de Seguridad Informática (cont.)

Documento 3: Políticas de Seguridad Informática (cont.)

Documento de Políticas de Seguridad Informática
16. Proteger los equipos para reducir los riesgos de las amenazas y peligros ambientales, y las oportunidades para el acceso no autorizado. 17. Proteger los equipos de fallas de energía y otras interrupciones causadas por fallas en los servicios públicos. 18. Proteger el cableado de la energía y las telecomunicaciones que llevan datos o sostienen los servicios de información deben ser protegidos de la intercepción o daño. **Encargado(a) de los activos debe:** 1. Identificar en forma clara los activos; y se debe elaborar y mantener un inventario de todos los activos importantes. 2. Toda la información y los activos asociados con los medios de procesamiento de la información deben tener asignado a un responsable. 3. Implementar, documentar e implementar las reglas para el uso aceptable de la información y los activos asociados con los medios de procesamiento de información. 4. Entregar a secretaría la documentación del inventario. 5. Clasificar la información con ayuda del Coordinador de Tecnología en términos de su valor, requerimientos legales, confidencialidad y grado crítico para la organización. 6. Desarrollar e implementar un apropiado conjunto de procedimientos para

Documento 3: Políticas de Seguridad Informática (cont.)

Documento 3: Políticas de Seguridad Informática (cont.)

Documento de Políticas de Seguridad Informática
etiquetar y manejar la información en concordancia con el esquema de clasificación de la organización. **Jefe de Talento Humano debe:** **Antes del empleo** 1. Definir y documentar los roles y responsabilidades de seguridad de los empleados, contratistas y terceros (padres de familia, estudiantes, personal temporal) referente a la seguridad de la información. 2. Llevar a cabo chequeos de verificación de antecedentes de todos los candidatos a empleados, contratistas y terceros en concordancia con las leyes, regulaciones y ética relevante, y deben ser proporcionales a los requerimientos comerciales, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos. 3. Establecer las responsabilidades y las de la organización para la seguridad de la información para los empleados contratistas y terceros como parte de su obligación contractual; (padres de familia, estudiantes, personal temporal) quienes deben aceptar y firmar los términos y condiciones de su contrato de empleo. **Durante el empleo (para padres de familia, entiéndase durante el tiempo o período académico que los estudiantes pasan en la Institución)** 1. Ver que todo el personal docente, administrativo del Centro Educativo y,

Documento 3: Políticas de Seguridad Informática (cont.)

Documento 3: Políticas de Seguridad Informática (cont.)

Documento de Políticas de Seguridad Informática
cuando sea relevante, los contratistas y terceros (padres de familia, estudiantes, personal temporal), deben recibir el apropiado conocimiento, capacitación y 2. actualizaciones regulares de las políticas y procedimientos organizacionales, conforme sean relevantes en su función laboral. 3. Mantener un proceso disciplinario formal para los empleados o terceros que han cometido violación en la seguridad establecido en el código de convivencia, y de acuerdo a lo estipulado en las Leyes de Educación, Código Laboral, Ley de Comercio Electrónico, Código Penal, entre otras. **Terminación o cambio de empleo** 1. Definir y asignar claramente las responsabilidades para realizar la terminación o cambio de empleo. 2. Garantizar que todos los empleados, contratistas, y terceros (padres de familia, estudiantes, personal temporal), deben devolver todos los activos de la organización que estén en su posesión a la terminación de su empleo, contrato o acuerdo. 3. Hacer el seguimiento para que los derechos de acceso de todos los empleados, contratistas y terceros (padres de familia, estudiantes, personal temporal) a la información y medios de procesamiento de la información, deben ser eliminados, o si fuera el caso pasar a un estado inactivo a la terminación de su empleo, contrato, acuerdo, o relaciones con el Centro Educativo. 4. Hacer el seguimiento para que los propietarios entreguen la clave del Deep

Documento 3: Políticas de Seguridad Informática (cont.)

Documento 3: Políticas de Seguridad Informática (cont.)

Documento de Políticas de Seguridad Informática
Freeze a la persona encargada de los Laboratorios (en caso de no existir asumirá las funciones el Profesor de Tics). **Coordinador de la seguridad informática debe:** 1. Monitorear el Plan de seguridad informática, en caso de que no esté creado, deberá crear un Plan de seguridad informática con su alcance y objetivos, el documento debe estar aprobado por la gerencia, debidamente registrado e identificado. 2. Mantener contacto con foros de seguridad o grupos de interés similares para estar pendiente de las novedades referente a vulnerabilidades y amenazas para la seguridad informática. 3. Apoyar activamente las auditorías que realicen los propietarios, para verificar el estado del Plan de Seguridad informática. 4. Notificar a los Propietarios y Dirección cualquier incidente de seguridad informático encontrado. La notificación debe ser por escrito o por correo electrónico, de lo contrario se asume que el incidente no fue reportado. 5. Estar en contacto con los proveedores de servicio de comunicaciones: Internet, Telefonía para reportar incidentes de fallos, interrupciones, daños. 6. Llevar una bitácora de incidentes de seguridad informática para análisis o futuras investigaciones de seguridad. 7. Colaborar con la persona encargada de Activos de la Institución para ayudar a

Documento 3: Políticas de Seguridad Informática (cont.)

Documento 3: Políticas de Seguridad Informática (cont.)

Documento de Políticas de Seguridad Informática
la asignación de propietarios de activos de información, de responsabilidades y obligaciones del Personal del Centro Educativo. 8. Ayudar a la persona encargada de Activos en la realización del inventario de activos de información cada año o cuando se considere necesario. 9. Estandarizar el uso de un único antivirus para toda la Institución. 10. Verificar que se actualice el antivirus de los equipos de los Laboratorios de Tics y del área Administrativa. 11. Verificar que se cumpla las políticas de: estandarización de software, protección física de hardware, redes, comunicaciones, respaldos. 12. Ver que se saquen y verifiquen los respaldos de la base de datos. 13. Respaldar los correos de incidencias reportadas, al igual que almacenar los documentos. 14. Informar por escrito de cualquier riesgo a los Propietarios y Dirección, que se evidencie ante una decisión tomada por ellos que tenga que ver con el área de tecnología. **Encargado de Tecnología** De no existir, asumirá las funciones el Profesor de Tics. 1. Firmar un documento de confidencialidad y buen recaudo de la integridad de los activos que maneja a la Institución. 2. Instalar el software base definido en los lineamientos de estandarización de software.

Documento 3: Políticas de Seguridad Informática (cont.)

Documento 3: Políticas de Seguridad Informática (cont.)

Documento de Políticas de Seguridad Informática
3. Mantener actualizado el antivirus y software base. 4. Chequear todos los ítems del equipo que contengan medios de almacenaje para asegurar que se haya removido o sobre-escrito de manera segura cualquier dato confidencial y software con licencia antes de su eliminación. 5. Encender los breakers al inicio de la jornada laboral 6. Encender los upses, equipos de comunicaciones, servidores todos los días antes de la jornada laboral y apagar los servidores después de la jornada laboral o cuando vea que haya tormenta eléctrica, incendio, descargas eléctricas, inundaciones, temblores. 7. Sacar respaldo de la base de datos y entregar a secretaría. 8. Manejar la clave del software Deep Freeze con seriedad y responsabilidad. 9. Informar de cualquier incidente de seguridad al Coordinador de la seguridad informática por escrito o por correo electrónico. 10. Bajar los breakers al final de la jornada laboral. **Personal Docente debe:** 11. Informar cualquier incidente de seguridad informática al Coordinador de seguridad informática por escrito o por correo electrónico. 12. Utilizar los recursos tecnológicos de la Institución exclusivamente para preparar clases, investigación, o como material de apoyo durante las clases. 13. Respetar las políticas de seguridad establecidas en la Institución. 14. Llenar el formulario de uso de los activos tecnológicos y presentarlo al

Documento 3: Políticas de Seguridad Informática (cont.)

Documento 3: Políticas de Seguridad Informática (cont.)

Documento de Políticas de Seguridad Informática
Coordinador de seguridad de la Información para hacer uso de los mismos para dar sus clases. Utilizar herramientas de búsqueda guiada (webquest, cazas de tesoro), si va a utilizar el Internet para que sus estudiantes hagan investigaciones o como material de apoyo en el aula. 15. Verificar que las páginas web a utilizar en sus clases tengan imágenes, videos, presentaciones que no incluyan pornografía, violencia, o cualquier cosa que pueda ser amenaza para la formación de los niños, niñas y adolescentes. 16. Capacitarse en el uso de Herramientas Tics en el aula periódicamente para mantener un elevado nivel tecnológico acorde con lo que los estudiantes manejan fuera de la Institución. **Personal Administrativo debe:** 1. Informar cualquier incidente de seguridad informática al Coordinador de seguridad informática por escrito o por correo electrónico. 2. Utilizar los recursos tecnológicos exclusivamente para el trabajo encomendado de la Institución. 3. Respetar las políticas establecidas en la Institución. 4. Realizar respaldos periódicos de la información que tiene a su cargo en el Servidor de Archivos. **Secretaría debe:** 1. Firmar un documento de confidencialidad y buen recaudo, de los respaldos que

Documento 3: Políticas de Seguridad Informática (cont.)

Documento 3: Políticas de Seguridad Informática (cont.)

Documento de Políticas de Seguridad Informática
tiene a su cargo en la institución. 2. Informar de cualquier incidente de seguridad informática al Coordinador de seguridad informática por escrito o por correo. 3. Apoyar al Coordinador de la seguridad informática para ayudar en la resolución de incidencias que tengan que ver con llamadas telefónicas, seguimiento a proveedores de servicios y registrar en una bitácora en la que se especifique: fecha, hora, incidencia, persona con quien habla, respuesta, número de incidencia (para proveedores de comunicaciones como telefonía, internet, etc.) e informar inmediatamente al coordinador de la seguridad informática vía correo electrónico o por escrito. 4. Guardar con orden y cautela todos los respaldos de todas las áreas, etiquetando y clasificando de tal forma que puedan ser encontrados y ubicados cuando se necesiten. 5. Copiar el respaldo global mensual con ayuda del Coordinador de Seguridad y entregar únicamente a los Propietarios con un documento por escrito que deberá archivarlo en una carpeta. **Padre de Familia debe:** 1. Informar cualquier incidente de seguridad informática que sea reportado por sus hijos(as) al Coordinador de Seguridad Informática por correo electrónico o por escrito.

Documento 3: Políticas de Seguridad Informática (cont.)

Documento 3: Políticas de Seguridad Informática (cont.)

Documento de Políticas de Seguridad Informática
2. Firmar un documento de compromiso con la institución responsabilizándose ante cualquier mal uso por parte de sus hijos (as) de los elementos tecnológicos de la Institución y la reposición inmediata en caso de daño intencionado. 3. Aportar con un valor designado por los propietarios y Dirección para mantenimiento de tecnología y uso de Internet. 4. Asistir a los talleres de Seguridad Informática que realice la Institución. **Estudiante debe:** 1. Informar sobre cualquier incidente de Seguridad Informática al Profesor de TICs o a su maestro. 2. Hacer buen uso de los activos tecnológicos y de información de la Institución. (para investigación, recibir clases, formación académica). Respetar las políticas de seguridad informática de la Institución.

Documento 3: Políticas de Seguridad Informática (Elaborado por: Investigador)

Acuerdo de confidencialidad

Documento de acuerdo de confidencialidad			
Fecha Emisión:	**Fecha Modificación:**	**Fecha de Aprobación:**	**Identificador** D-SEC-02
Elaborado por:		**Revisado y Aprobado por:**	

I. INTRODUCCIÓN

El presente documento define el acuerdo de confidencialidad establecido entre el Centro Educativo La Pradera y …….”

II. ACUERDO DE CONFIDENCIALIDAD

Entre los suscritos a saber, por una parte Centro Educativo La Pradera constituido bajo las leyes del Ecuador con domicilio en la ciudad de Sangolquí, debidamente representada por su Representante Legal y Director Arquitecto Luis Atapuma, mayor de edad y domiciliado en la ciudad de Sangolquí, identificando como aparece al pie de su respectiva firma; y por la otra, ……, también mayor de edad y domiciliado(a) en la ciudad de ……, identificado(a) como aparece al pie de su firma, quien actúa en nombre de ……, se ha acordado celebrar el presente Acuerdo de Confidencialidad que se regirá por las siguientes cláusulas, previas las siguientes:

CONSIDERACIONES

1. Las partes están interesadas en ……..
2. Debido a la naturaleza del trabajo, se hace necesario que éstas manejen información confidencial y/o información sensible de estudiantes, respaldos antes, durante y en la etapa posterior.

CLÁUSULAS

PRIMERA. OBJETO. El objeto del presente acuerdo es fijar los términos y condiciones bajo los cuales las partes mantendrán la confidencialidad de los datos e información intercambiados entre ellas, incluyendo información objeto de respaldos, proyectos, documentos históricos, información financiera, lista de estudiantes con sus calificaciones, empleados, relaciones de negocios y

Documento 4: Documento de acuerdo de confidencialidad (cont.)

Documento 4: Documento de acuerdo de confidencialidad (cont.)

Documento de acuerdo de confidencialidad
contractuales, y cualquier información revelada sobre terceras personas. **SEGUNDA. CONFIDENCIALIDAD.** Las partes acuerdan que cualquier información intercambiada, facilitada o creada entre ellas en el transcurso de ……, será mantenida en estricta confidencialidad a quienes la necesiten y estén autorizados previamente por la parte de cuya información confidencial se trata. Se considera también información confidencial: a) Aquella que como conjunto o por la configuración o estructuración exacta de sus componentes, no sea generalmente conocida entre los expertos en los campos correspondientes, b) La que no sea de fácil acceso, y c) Aquella información que no esté sujeta a medidas de protección razonables, de acuerdo con las circunstancias del caso, a fin de mantener su carácter confidencial. **TERCERA. EXCEPCIONES.** No habrá deber alguno de confidencialidad en los siguientes casos: a) Cuando la parte receptora tenga evidencia de que conoce previamente la información recibida; b) Cuando la información recibida sea de dominio público y, c) Cuando la información deje de ser confidencial por ser revelada por el Propietario. **CUARTA. DURACIÓN.** Este acuerdo regirá durante el tiempo que dure …… hasta un término de tres años contados a partir de su fecha. **QUINTA. DERECHOS DE PROPIEDAD.** Toda información intercambiada es de propiedad exclusiva de la parte donde proceda. En consecuencia, ninguna de las partes utilizará información de la otra para su propio uso. **SEXTA. MODIFICACIÓN O TERMINACIÓN**. Este acuerdo solo podrá ser modificado o darse por terminado con el consentimiento expreso por escrito de ambas partes.

Documento 4: Documento de acuerdo de confidencialidad (cont.)

Documento 4: Documento de acuerdo de confidencialidad (cont.)

Documento de acuerdo de confidencialidad
SÉPTIMA. VALIDEZ Y PERFECCIONAMIENTO. El presente Acuerdo requiere para su validez y perfeccionamiento la firma de las partes. Si cualquier disposición de este Acuerdo fuera juzgada por una corte competente como nula o ilegal, las demás disposiciones continuarán en pleno vigor y efecto. Todas las obligaciones creadas por este Acuerdo continuarán en vigencia aún después de cualquier cambio o terminación de la relación profesional existente entre las partes. Para constancia, y en señal de aceptación, se firma el presente acuerdo en ejemplares, por las partes que en él han intervenido, en la ciudad de Sangolquí a los…….() días del mes de ……. de …….(201_). _____ _____ Documento de Identidad Documento de Identidad

Documento 4: Acuerdo de confidencialidad (Fuente: (Chamorro, V., 2013, págs. 97-99)) (Elaborado por Investigador)

Uso aceptable de los activos de información

Documento para uso aceptable de los Activos informáticos			
Fecha de Emisión:	**Fecha de Modificación:**	**Fecha de Aprobación**	**Identificador** L-COR-02
Elaborado por:		**Revisado por:**	

- **INTRODUCCIÓN**

Este documento detalla las responsabilidades que tendrán el personal docente, administrativo, tecnología, estudiantes, padres de familia del Centro Educativo La Pradera.

- **ASIGNACIÓN DE RESPONSABILIDADES**

Las responsabilidades quedan distribuidas de la siguiente manera:

El Centro Educativo La Pradera requiere que los activos de apoyo sean utilizados de una manera aceptable. El correcto uso de los mismo se define en los siguientes párrafos:

LINEAMIENTO PARA USO DE CORREO

- El Centro educativo La Pradera deberá disponer de las siguientes cuentas de correo electrónico para:

Área	**Administra**
Institución	Secretaria
Secretaría	Secretaria

Documento 5: Uso aceptable de los activos de información (Elaborado por: Investigador) (cont.)

Documento 5: Uso aceptable de los activos de información (cont.)

Documento para uso aceptable de los Activos informáticos

Área	Administra
Inspección	Inspectora
Dove	Psicóloga educativa
Coordinación académica	Coordinador académica
Dirección	Director(a) de la Institución
Tecnología	Coordinador de la Seguridad Informática

- Es responsabilidad de los usuarios hacer un buen uso de las cuentas de la Institución, entendiendo por buen uso:
- El no mandar ni contestar cadenas de correo.
- El uso de su cuenta con fines académicos y/o investigación
- El uso de un lenguaje apropiado en sus comunicaciones.
- Es responsabilidad del usuario cambiar sus contraseña con regularidad
- El usuario será responsable de la información que sea enviada con su cuenta, por lo cual se asegurará de no mandar SPAMS de información, ni anexos que pudieran contener información nociva para otro usuario como virus o pornografía.
- El usuario es responsable de respaldar sus archivos de correo.

LINEAMIENTO DEL USO DE INTERNET

- Será posible hacer uso de la red Internet:

Para el personal Docente:

Únicamente para preparar material de apoyo para sus clases, para investigación, o fines consultivos, ingreso al sistema de gestión del Centro Educativo La Pradera.

Documento 5: Uso aceptable de los activos de información (Elaborado por: Investigador) (cont.)

Documento 5: Uso aceptable de los activos de información (cont.)

Documento para uso aceptable de los Activos informáticos
Para los estudiantes: Únicamente en el Laboratorio de TICs, en tareas encomendadas por sus Profesores, tareas que contribuyan a una formación sana y segura. **Para el personal Administrativo**: Únicamente para tareas propias del trabajo, fines consultivos, definiéndose como consultivo a todas aquellas búsquedas de información que apoyen al usuario a resolver un problema o inconveniente. • El encargado de tecnología junto con el encargado de los activos será el encargado de asignar una máquina al usuario, quién será responsable durante el tiempo que permanezca en su poder. • El Centro Educativo La Pradera se reserva el derecho de revisión de los equipos en cualquier momento para revisar la información almacenada en los discos duros de los equipos. • Cualquier uso que cause efectos opuestos a la operación del Centro Educativo La Pradera o ponga en riesgo el uso o rendimiento de la red, será analizado por los Propietarios y Dirección para tomar medidas. • En caso de usar utilizar el Sistema de Gestión de Información del Centro Educativo La Pradera en Internet se debe asegurar de salir cerrando todas las sesiones abiertas.

Documento 5: Uso aceptable de los activos de información (Elaborado por: Investigador) (cont.)

Documento 5: Uso aceptable de los activos de información (cont.)

Documento para uso aceptable de los Activos informáticos
LINEAMIENTOS PARA USO DE EQUIPOS • Cuando exista la necesidad de sacar un equipo fuera del Centro Educativo La Pradera se debe tener autorización del Coordinador de la Seguridad Informática y de los Propietarios con la respectiva nota de entrega. • No es permitido que los usuarios utilicen equipos del Centro Educativo La Pradera para asuntos personales (como alquiler a terceros, pruebas personales, entre otros). • Cuando alguien salga con equipos, es necesario disponer de transporte seguro ya sea propio o puede ser un servicio de taxis a domicilio. **LINEAMIENTO PARA USO DE DOCUMENTOS** • En el Centro Educativo La Pradera existe documentación del Sistema de Gestión de Información, la misma que es manejada por el Propietario y una copia reposa en secretaría, que puede ser utilizada dentro de la Institución. • En caso de ser necesario sacar documentación de manuales del área de tecnología fuera del Centro Educativo La Pradera se debe notificar de este hecho al Coordinador de la Seguridad Informática mediante un correo electrónico. Si el documento está en digital se aplicará el acuerdo de confidencialidad. **LINEAMIENTO PARA USO DE RED INALÁMBRICA** • El Centro Educativo La Pradera dispone de una red inalámbrica para la cual podrán solicitar acceso al Coordinador de la seguridad informática. • El usuario y clave de la red inalámbrica estará bajo la custodia del Coordinador de la seguridad informática.

Documento 5: Uso aceptable de los activos de información (Elaborado por: Investigador) (cont.)

Documento 5: Uso aceptable de los activos de información (cont.)

Documento para uso aceptable de los Activos informáticos
LINEAMIENTO PARA CONTROL DE ACCESO A REDES La red del Centro Educativo La Pradera deberá ser administrada por la Persona encargada de tecnología y deberá realizar las siguientes tareas: • Crear usuarios • Asignación de Permisos • Compartición de recursos en red (carpetas, archivos, impresoras) • Desbloqueo de usuarios • Actualización de contraseñas • Respaldar la información del servidor de archivos • Revisar que el antivirus de los servidores esté actualizado. • Revisar los logs de los servidores para poder identificar posibles alertas o errores, fallos en el funcionamiento de alguno de los servicios. • Revisar procesos activos para identificar procesos inusuales que estén trabajando. • Revisar el consumo de recursos. • Revisar e instalar las actualizaciones que sean necesarias para el sistema operativo de los servidores. • Tener un servidor de respaldo para contingencias. • Realizar pruebas periódicas del funcionamiento adecuado de los respaldos • Ver que los niveles de servicio de los servidores: servidor de archivos, servidor de usuarios, servidor de correo, servidor de transferencia de archivos (ftp), servidor web (externo), proxy, firewall estén funcionando en óptimas condiciones.

Documento 5: Uso aceptable de los activos de información (Elaborado por: Investigador) (cont.)

Documento 5: Uso aceptable de los activos de información (cont.)

Documento para uso aceptable de los Activos informáticos
LINEAMIENTO PARA CONTROL DE ACCESO A INTERNET • El Centro Educativo La Pradera dispone de un Firewall y un servidor proxy para el control y restricción de acceso a Internet, el mismo que será administrado por el Encargado de Tecnología. • El Firewall trabajará de manera restrictiva de tal forma que la persona encargada de su administración deberá habilitar de acuerdo a las necesidades de la Institución. • Autorizará el acceso el Coordinador de la Seguridad Informática previa solicitud entregada. **LINEAMIENTO PARA USO DE SOFTWARE** • Se deberá utilizar el software base instalado en los equipos que a continuación se especifica: **Laboratorios** • Sistema Operativo: Windows 7 • Antivirus: Avast free • Software Deep freeze • Herramientas Ofimáticas: Open Office • Navegadores: Firefox • Visor de Archivos pdf Acrobat • Adobe Flash Player • Gran Caco (Inglés) • Software libre para Matemáticas y otras áreas

Documento 5: Uso aceptable de los activos de información (Elaborado por: Investigador) (cont.)

Documento 5: Uso aceptable de los activos de información (cont.)

Documento para uso aceptable de los Activos informáticos
Área Administrativa • Sistema Operativo: Windows 7 • Antivirus: Avast free • Herramientas Ofimáticas: Open Office • Visor de archivos pdf Acrobat • Navegador: Firefox, Internet Explorer • Adobe Flash Player • Sistema de Gestión de Información • Software DIMM (únicamente para el equipo que utiliza el contador) **Sala de Docentes** Lo mismo que el personal administrativo y adicional: • Windows media player • Software libre Jclic • Cualquier herramienta de software libre que permita la creación de material de apoyo para los estudiantes previa autorización del Coordinador de Seguridad informática. • Por ningún motivo se podrá instalar software adicional sin la autorización del Coordinador de la Seguridad informática. • En caso de requerir instalar software adicional deberá ser de uso libre y será necesario solicitar por correo o por escrito al Coordinador de la Seguridad informática su autorización. • Será responsabilidad del Encargado de Tecnología mantener actualizado dicho software.

Documento 5: Uso aceptable de los activos de información (Elaborado por: Investigador) (cont.)

Documento 5: Uso aceptable de los activos de información (cont.)

Documento para uso aceptable de los Activos informáticos
LINEAMIENTO PARA REALIZACIÓN DE RESPALDOS • Respaldar la base de datos todos los días y al final de la jornada laboral y entregar a secretaría una copia del respaldo. • Respaldar la información de secretaría en el disco duro externo y en un disco virtual (Dropbox). • Respaldar la información de inspección en un dvd y entregar a secretaría. • Respaldar la información del encargado(a) de los activos y entregar a secretaría. • Respaldar la información de proyectos elaborados por los docentes y entregar a secretaría. • Realizar una copia mensual de todos los respaldos y entregar a los propietarios para que la guarden en un lugar fuera de la Institución. **LINEAMIENTO PARA TRABAJAR CON ESTUDIANTES** • El Centro Educativo La Pradera tiene como proceso de negocio principal la Formación de niños, niñas y adolescentes, es así que al trabajar con los estudiantes usando herramientas de apoyo de Internet, se debe utilizar herramientas guiadas (webquest o caza de tesoro) . • Verificar que las páginas a las que van a acceder no tengan algún tipo de amenaza. • Probar los activos tecnológicos a ser utilizados antes de dictar la clase. • Las comunicaciones, servidores, medios tienen que estar en correcto funcionamiento. • Monitorear mientras los estudiantes reciben clases.

Documento 5: Uso aceptable de los activos de información (Elaborado por: Investigador) (cont.)

Documento 6: Uso aceptable de los activos de información (Elaborado por: Investigador) (cont.)

Documento para uso aceptable de los Activos informáticos
LINEAMIENTO PARA USO DE CLAVES DE USUARIOS • La clave es de uso personal y no debe ser prestada. • La clave deberá ser cambiada una vez al mes. • Los caracteres de la clave deberán ser alfanuméricos de 8 a 10 caracteres mínimo, tener una combinación de números, letras y símbolos y no deben estar relacionadas con datos personales del usuario. • En caso de olvido de clave deberá contactarse con el Encargado de tecnología para que le ayude a gestionar una nueva contraseña. En caso de sospecha de que la contraseña es conocida por terceros deberá reportar al Coordinador de Seguridad Informática para que registre el incidente e investigue el origen del mismo y solicitar al Encargado de tecnología que le ayude a gestionar una nueva contraseña.

Documento 5: Uso aceptable de los activos de información

(Elaborado por: Investigador) (Fuente: (Chamorro, V., 2013, págs. 107-110))

Instructivo para nombrar respaldos

Instructivo para nombrar respaldos			
Fecha Emisión:	**Fecha Modificación:**	**Fecha de Aprobación:**	**Identificador I-SEC-02**
Elaborado por:		**Revisado y Aprobado por:**	

I. INTRODUCCIÓN

Este instructivo permite que los respaldos mantengan un estándar y sean de fácil reconocimiento para quien los maneje.

II. PROCEDIMIENTO PARA REALIZAR EL RESPALDO

1. Los respaldos deberán ser nombrados con el siguiente formato: los tres primeros caracteres alfanuméricos corresponderán al área a la que pertenecen,

Iniciales	**Área**
SEC	Secretaría
INS	Inspección
LAB	Laboratorio TICs
DIR	Dirección
PRO	Propietarios
SOF	Software
TEC	Encargado de Tecnología
COR	Coordinador de la Seguridad Informática
DOC	Personal Docente
ADM	Personal Administrativo
DOV	DOVE
ACA	Coordinación Académica

Documento 6: Instructivo para nombrar respaldos (Elaborado por: Investigador) (cont.)

Documento 6: Instructivo para nombrar respaldos (cont.)

Instructivo para nombrar respaldos

El siguiente dígito es '-', los 2 siguientes caracteres alfanuméricos corresponderán al tipo de documento

Iniciales	Tipo
CO	Comunicados
OF	Oficios
AC	Actas
DR	Documentos recibidos
PR	Proyectos
MA	Manuales
BD	Base de datos
PE	Pensiones
De	Declaraciones
CA	Calificaciones

El siguiente dígito es '-', los tres siguientes dígitos muestran el orden secuencial del documento.

Para el caso de Proyectos se añadirá '-'seguido de 5 caracteres alfanuméricos que identifique el nombre del proyecto.

Para la base de datos se añadirá '-'seguido del año-mes-día.

Documento 6: Instructivo para nombrar respaldos (Elaborado por: Investigador)

Instructivo para el inventario de activos

Instructivo para el Inventario de Activos			
Fecha Emisión:	**Fecha Modificación:**	**Fecha de Aprobación:**	**Identificador I-INS--03**
Elaborado por:		**Revisado y Aprobado por:**	

I. INTRODUCCIÓN

Este instructivo permite realizar el inventario de activos de información del Centro Educativo La Pradera.

II. PROCEDIMIENTO PARA REALIZAR EL INVENTARIO

Todos los activos deben ser registrados en el siguiente formato de tabla donde muestra las características que se deben tomar en cuenta de cada activo.

Identificación	Tipo	Activo	Descripción	Propietario	Ubicación física

Documento 7: Instructivo para el Inventario de Activos (Elaborado por: Investigador)

Formato para solicitar salida de equipos fuera del CELP

Formato de salida de equipos fuera del CELP			
Fecha de emisión:	**Fecha Modificación:**	**Fecha de Aprobación:**	**Identificador F-COR-01**
Elaborado por:		**Revisado y Aprobado por:**	

I. INTRODUCCIÓN

Este documento tiene el formato para solicitar salida de equipos fuera del Centro Educativo La Pradera.

II. FORMATO

Solicita:	**Aprueba:**
Fecha: **Solicita:** **Cliente:** **Fecha de préstamo:** **Fecha de devolución:** **Motivo de préstamo:** **Revisado por:**	**Pedido #:** **Días aproximados:** **Autorizado por:**
Observaciones:	

Listado de Equipos			
Código	**Equipo**	**Descripción**	**Cantidad**
Atentamente		**Recibí conforme**	

Documento 8: Formato para solicitar salida de equipos fuera del CELP (Elaborado por: Investigador)

Formato de devolución de equipos

Formato de devolución de equipos			
Fecha de emisión:	**Fecha de modificación**	**Fecha de aprobación**	**Identificador** **F-COR-02**
Elaborado por:		**Revisado y aprobado por:**	

I. INTRODUCCIÓN

Este documento tiene el formato para realizar la devolución de equipos al Centro Educativo La Pradera.

II. FORMATO

Fecha: **Atención:** **Cliente:** **Fecha de préstamo:** **Fecha de devolución:**	**Entrega #:** **Pedido #:** **Días aproximados:**

Observaciones:

Sírvase encontrar adjunto a la presente lo siguiente:

Código	**Equipo**	**Descripción**	**Cantidad**
Atentamente		**Recibí conforme**	

Documento 9: Formato de devolución de equipos (Elaborado por: Investigador)

Formato de solicitud de acceso a sitios web

Formato de Solicitud de acceso a sitios web			
Fecha de emisión:	**Fecha de modificación:**	**Fecha de aprobación:**	**Identificador F-COR-03**
Elaborado por:		**Revisado y aprobado por:**	

I. INTRODUCCIÓN

Este documento tiene el formato para solicitar acceso a sitios web en el Centro Educativo La Pradera.

II. FORMATO

Fecha:	**Solicitud #:**
Nombre de quien solicita:	**Autorizado por:**
Observaciones:	

Páginas a las que solicita acceso			
Dirección de la página	**Equipos**	**Período**	**Justificación**
Atentamente		**Recibí conforme**	

Documento 10: Formato de Solicitud de acceso a sitios web (Elaborado por: Investigador)

Formato de solicitud de reparación de equipo de usuario desatendido

<table>
<tr><td colspan="4">Formato de Solicitud de reparación de equipo de usuario desatendido</td></tr>
<tr><td>Fecha de emisión:</td><td>Fecha de modificación:</td><td>Fecha de aprobación:</td><td>Identificador
F-COR-04</td></tr>
<tr><td colspan="2">Elaborado por:</td><td colspan="2">Revisado y aprobado por:</td></tr>
<tr><td colspan="4">I. INTRODUCCIÓN
Este documento tiene el formato para solicitar de algún equipo desatendido en el Centro Educativo La Pradera.
II. FORMATO</td></tr>
<tr><td colspan="2">Fecha:
Hora:
Nombre de quien solicita:</td><td colspan="2">Solicitud #:
Autorizado por:</td></tr>
<tr><td colspan="4">Observaciones:</td></tr>
<tr><td colspan="2">Atentamente</td><td colspan="2">Recibí conforme</td></tr>
</table>

Documento 11: Formato de Solicitud de reparación de equipo de usuario desatendido (Elaborado por: Investigador)

Instructivo para revisión de políticas de seguridad informática

Instructivo para revisión de políticas de seguridad informática			
Fecha de emisión:	**Fecha de modificación:**	**Fecha de aprobación:**	**Identificador I-DIR-04**
Elaborado por:		**Revisado y aprobado por:**	

I. INTRODUCCIÓN

Este instructivo sirve para evaluar la revisión de las políticas de seguridad informática implementadas en el Centro Educativo La Pradera.

II. REVISIÓN DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA

Se debe revisar cada política de seguridad informática implementada en el Centro Educativo La Pradera y marcar la efectividad de la misma, así como detallar alguna observación.

Política	Efectividad				Observación
	Excelente	Buena	Mala	Pésima	

Documento 12: Instructivo para revisión de políticas de seguridad informática (Elaborado por: Investigador) (cont.)

Documento 12: Instructivo para revisión de políticas de seguridad informática (cont.)

Instructivo para revisión de políticas de seguridad informática
En caso de existir documentación de incidentes de seguridad informática relativo con las políticas, se debe tomar en cuenta para evaluar la política y debe registrarse la observación respectiva. Firman Revisores _____ _____ PROPIETARIO DIRECCIÓN _____ _____ RECURSOS HUMANOS COORD. ACADEMICA _____ _____ COORDINADOR DE SEGURIDAD INFORMÁTICA ENCARGADO DE TECNOLOGÍA _____ _____ REPRESENTANTE DE LOS DOCENTES REPRESENTANTE DE PADRES DE FAMILIA _____ REPRESENTANTE DE LOS ESTUDIANTES

Documento 12: Instructivo para revisión de políticas de seguridad informática (Elaborado por: Investigador) (Fuente: (Chamorro, V., 2013, pág. 116))

Instructivo para segregación de redes

Instructivo para segregación de redes			
Fecha de emisión:	**Fecha de modificación:**	**Fecha de aprobación:**	**Identificador I-TEC-05**
Elaborado por:		**Revisado y aprobado por:**	

I. INTRODUCCIÓN

El Centro Educativo La Pradera maneja un esquema de red jerárquica por capas: capa de acceso, capa de distribución, capa de núcleo.

II. INSTRUCTIVO

l. Las redes estarán divididas de la siguiente forma:

Red de Laboratorio Bloque 2

Red de Laboratorio Bloque 1

Red Bloque 3

2. Las direcciones IP asignadas a cada red deberán ser asignadas de acuerdo a la siguiente tabla:

Direccionamiento				
Bloque 1		**Equipos**	**Ips**	**Máscara**
Laboratorio Bloque 1: 192.168.4.0	Cuarto de comunicaciones	Servidor Proxy - firewall	192.168.6.100	255.255.255.0
		Switch Capa 3- Bloque 1	192.168.6.101	255.255.255.0
		Switch Capa 3- Bloque 3	192.168.6.102	255.255.255.0
		Switch Capa 3 - Servidores	192.168.6.103	255.255.255.0
		Router Wireless Administrativo	192.168.6.104	255.255.255.0

Documento 13: Instructivo para segregación de redes (Elaborado por: Investigador) (cont.)

Documento 13: Instructivo para segregación de redes (cont.)

Instructivo para segregación de redes				
Direccionamiento				
Bloque 1		**Equipos**	**Ips**	**Máscara**
Laboratorio Bloque 1 192.168.4.0	Cuarto de comunicaciones	Router Wireless Laboratorio	192.168.6.105	255.255.255.0
		Servidor de Aplicaciones	192.168.6.106	255.255.255.0
		Servidor de autenticación red inalámbrica	192.168.6.107	255.255.255.0
	Estudiantes	LAB_B1_01	192.168.4.1	255.255.255.0
		LAB_B1_02	192.168.4.2	255.255.255.0
		LAB_B1_03	192.168.4.3	255.255.255.0
		LAB_B1_04	192.168.4.4	255.255.255.0
		LAB_B1_05	192.168.4.5	255.255.255.0
		LAB_B1_06	192.168.4.6	255.255.255.0
		LAB_B1_07	192.168.4.7	255.255.255.0
		LAB_B1_08	192.168.4.8	255.255.255.0
		LAB_B1_09	192.168.4.9	255.255.255.0
		LAB_B1_10	192.168.4.10	255.255.255.0
		LAB_B1_11	192.168.4.11	255.255.255.0
		LAB_B1_12	192.168.4.12	255.255.255.0
		LAB_B1_13	192.168.4.13	255.255.255.0
		LAB_B1_14	192.168.4.14	255.255.255.0
		LAB_B1_15	192.168.4.15	255.255.255.0

Documento 13: Instructivo para segregación de redes (Elaborado por: Investigador) (cont.)

Documento 13: Instructivo para segregación de redes (cont.)

Instructivo para segregación de redes

Tabla de Direccionamiento Bloque 2

Bloque 2		**Equipos**	**Ips**	**Máscara**
Proyección Laboratorio Bloque 2 192.168.5.0	Estudiantes	LAB_B2_01	192.168.5.1	255.255.255.0
		LAB_B2_02	192.168.5.2	255.255.255.0
		LAB_B2_03	192.168.5.3	255.255.255.0
		LAB_B2_04	192.168.5.4	255.255.255.0
		LAB_B2_05	192.168.5.5	255.255.255.0
		LAB_B2_06	192.168.5.6	255.255.255.0
		LAB_B2_07	192.168.5.7	255.255.255.0
		LAB_B2_08	192.168.5.8	255.255.255.0
		LAB_B2_09	192.168.5.9	255.255.255.0
		LAB_B2_10	192.168.5.10	255.255.255.0

Tabla de Direccionamiento Bloque 3

Bloque 3		**Equipos**	**Direccionamiento**	**Máscara**
		Secretaría	192.168.3.2	255.255.255.0
		DOBE	192.168.3.3	255.255.255.0
		Inspección	192.168.3.4 - 192.168.3.8	255.255.255.0
		Dirección	192.168.3.9	255.255.255.0
		Sala de Docentes	192.168.3.10 - 192.168.3.16	255.255.255.0
		Propietarios	192.168.3.17	255.255.255.0
Red Inalámbrica: 192.168.2.0	Invitados	Invitados, Docentes-Autoridades	192.168.2.1 - 192.168.2.40	255.255.255.0

Documento 13: Instructivo para segregación de redes (Elaborado por: Investigador)

Instructivo de switching, routing de redes

Instructivo de Switching y Routing de redes			
Fecha de emisión:	**Fecha de modificación:**	**Fecha de Aprobación:**	**Identificador I-TEC-06**
Elaborado por:		**Revisado y aprobado por:**	

I. INTRODUCCIÓN

El Centro Educativo La Pradera maneja un esquema de red jerárquica para lo cual se usa tecnología de switching y routing.

II. INSTRUCTIVO

1. Los switches de la capa de acceso van conectados a los switches de la capa de distribución: switch Bloque 1 (proyección), switch Bloque 2, switch Bloque 3.
2. Los Switches de la capa de distribución (administrables) van conectados entre sí por el puerto escalable, además de conectarse switch de servidores de la capa de núcleo.
3. El router va conectado al Switch de servidores de la capa de núcleo
4. El Switch de servidores va conectado a los swithes de la capa de distribución; Switch Bloque1 (proyección), Switch Bloque2, Switch Bloque 3.

Documento 14: Instructivo de switching y routing de redes (Elaborado por: Investigador)

Registro de Compromiso de los Propietarios y Dirección con la Seguridad Informática

Registro de Compromiso de los Propietarios y Dirección con la Seguridad Informática			
Fecha de emisión:	**Fecha de modificación:**	**Fecha de Aprobación:**	**Identificador R-PRO-01**
Elaborado por:		**Revisado y aprobado por:**	

I. INTRODUCCIÓN

Este documento permite el registro del compromiso que Propietarios y la Dirección establecen con el Plan de Seguridad de Informática a implementarse en el Centro Educativo La Pradera.

II. COMPROMISO DE LOS PROPIETARIOS Y LA DIRECCIÓN CON EL PLAN DE SEGURIDAD INFORMÁTICA

Los propietarios y la Dirección del Centro Educativo La Pradera ha leído y se encuentra consciente cuán importante es el establecimiento de políticas de seguridad informática en la Institución.

Es por esto que los Propietarios y Dirección manifiestan el compromiso y el apoyo activo para con el proyecto de implementación de las políticas de seguridad informática.

Los Propietarios y la Dirección pueden intervenir en el desarrollo e implementación de las políticas, incluso pueden dar por terminado el desarrollo de la implementación en caso de considerarlo necesario.

Firman

_____ _____

Propietarios Dirección

Documento 15: Registro de Compromiso de los Propietarios y Dirección con la Seguridad Informática (Elaborado por: Investigador)

Reporte de incidentes de seguridad informática

Documento de Reporte de Incidentes de seguridad informática			
Fecha de emisión:	**Fecha de modificación:**	**Fecha de Aprobación:**	**Identificador** **R-COR-02**
Elaborado por:		**Revisado y aprobado por:**	

I. INTRODUCCIÓN

Este documento permite reportar las incidencias al Coordinador de Seguridad Informática.

II. Registro

Nombre de quien reporta: …….

Fecha: ……

Incidente: ……..

……

……

……

…….

Firma Firma

_____ _____

Quien reporta Coordinador de seguridad de la información

Documento de identidad Documento de identidad

Documento 16: Reporte de Incidentes de seguridad informática (Elaborado por: Investigador)

Registro de incidencias reportadas a los proveedores de Telecomunicaciones

Documento de Registro de Incidencias reportadas a los proveedores de Telecomunicaciones			
Fecha de emisión:	**Fecha de modificación:**	**Fecha de Aprobación:**	**Identificador** **R-COR-03**
Elaborado por:		**Revisado y aprobado por:**	

I. INTRODUCCIÓN

Este documento permite registrar las incidencias reportadas a los proveedores de Telecomunicaciones.

II. Registro

Se debe registrar las incidencias de: daños, cortes de telefonía e Internet

TIPO **(T telefonía, I internet)**	**Fecha de reporte**	**Nombre de quien reporta**	**Persona que atiende**	**Descripción de** **Incidencia**	**# de Incidencia** **(proporciona el proveedor)**	**Observaciones** **(Descripción de lo que le dice que haga la persona que atiende la incidencia)**

Documento 17: Registro de incidencias reportadas a los proveedores de Telecomunicaciones (Elaborado por: Investigador)

Registro de reparación de equipo de usuario desatendido

Registro de Incidencias de equipos de usuarios desatendidos			
Fecha de emisión:	**Fecha de modificación:**	**Fecha de aprobación:**	**Identificador** **R-TEC-04**
Elaborado por:		**Revisado y aprobado por:**	

I. INTRODUCCIÓN

Este documento permite registrar las incidencias de los equipos de usuarios desatendidos y estará a cargo del Encargado de Tecnología.

II. REGISTRO DE INCIDENCIAS DE EQUIPOS DE USUARIOS DESATENDIDOS

Fecha	Hora	Usuario	Equipo	Solicitud #	Problema reportado	Solución	Fecha de solución

Documento 18: Registro de reparación de equipos de usuarios desatendidos (Elaborado por: Investigador)

Documento de entrega de respaldos a los Propietarios

Documento de entrega de Respaldos a los Propietarios			
Fecha de emisión:	**Fecha de modificación:**	**Fecha de Aprobación:**	**Identificador** **R-SEC-04**
Elaborado por:		**Revisado y aprobado por:**	

III. INTRODUCCIÓN

Este documento permite registrar la entrega de Respaldos de la información general por parte de Secretaría, mensuales a los Propietarios de la Institución, los mismos que deberán ser mantenidos fuera de la misma.

IV. TEXTO

Fecha: …….

Hora: ……

Por medio del presente documento hago la entrega de una copia de la información siguiente:

- Respaldos diarios de la base de datos
- Información histórica del Centro Educativo La Pradera
- Información del presente año lectivo de Secretaría
- Información del presente año lectivo de Inspección
- Proyectos elaborados por los el personal Docente y Administrativo
- …… (se escribirá cualquier documentación adicional que no esté especificada, añadiendo los ítems que se requieran)

Firma Firma

_____ _____

SECRETARIA PROPIETARIO

Documento de identidad Documento de identidad

Documento 19: Documento de entrega de respaldos a los propietarios (Elaborado por: Investigador)

Reporte de incidencias de seguridad informática a los Propietarios y Dirección

Formato de Reporte de incidentes de seguridad informática a los Propietarios y Dirección			
Fecha de emisión:	**Fecha de modificación:**	**Fecha de Aprobación:**	**Identificador** **F-COR-05**
Elaborado por:		**Revisado y aprobado por:**	

I. INTRODUCCIÓN

Este documento es un registro de haber reportado incidencias de seguridad informática a los Propietarios y Dirección

II. REPORTE DE INCIDENCIAS:

Fecha	Hora	#Incidencia	Quien reporta	Solución	Observaciones

Firma Firma

_____ _____ _____

Quien reporta Propietario Dirección

Documento de identidad Documento de identidad Documento de identidad

Documento 20: Reporte de incidencias de seguridad informática a los Propietarios y Dirección (Elaborado por: Investigador)

Registro de Contacto con grupos de seguridad informática

Registro de Contacto con grupos de seguridad informática			
Fecha de emisión:	**Fecha de modificación:**	**Fecha de Aprobación:**	**Identificador** **R-COR-05**
Elaborado por:		**Revisado y aprobado por:**	

III. INTRODUCCIÓN

Este documento permite verificar que el Coordinador de la seguridad informática ha tenido contacto con grupos de seguridad informática.

IV. REGISTRO DE CONTACTO

Fecha	Hora	Tema tratado	Tipo (Foro /Taller) o Fuente de información

Documento 21: Registro de contacto con grupos de seguridad informática (Elaborado por: Investigador)

Registro de Contacto con las autoridades

Registro de Contacto con las autoridades			
Fecha de emisión:	**Fecha de modificación:**	**Fecha de Aprobación:**	**Identificador** **R-COR-06**
Elaborado por:		**Revisado y aprobado por:**	

I. INTRODUCCIÓN

Este documento es un registro de haber tenido contacto con los Propietarios y la Dirección acerca del Plan de Seguridad de la Informática.

II. TEMAS TRATADOS:

A continuación se especifican los temas mencionados con las autoridades.

Documento 22: Registro de Contacto con las autoridades (Elaborado por: Investigador)

Formato de uso de activos tecnológicos

Formato de uso de activos tecnológicos			
Fecha Emisión:	**Fecha Modificación:**	**Fecha de Aprobación:**	**Identificador** **F-TEC-06**
Elaborado por:		**Revisado y Aprobado por:**	

I. INTRODUCCIÓN

Este documento es un Formato de uso de activos tecnológicos para ser usado para solicitar los mismos dentro del CELP.

II. FORMATO

Solicita: _____

Fecha de préstamo: _____ **Hora de préstamo:** _____

Fecha de entrega: _____ **Hora de entrega:** _____

Asignatura: _____ **Tema a tratar:** _____

_____

ACTIVO	✖ √	OBSERVACIÓN
Internet	_____	_____
Laboratorio	_____	_____
Proyector	_____	_____
Portátil	_____	_____
Computador	_____	_____

_____

Firma Autoriza Solicita

_____ _____ _____

Encargado de Tecnología Coordinador(a) Académico(a) CI.

Documento 23: Formato de uso de activos tecnológicos (Elaborado por: Investigador)

6.8.3 Rediseño de la Red

6.8.3.1 **Análisis de Requerimientos**

Ubicación: Sangolquí

Gráfico: 6.10 Mapa Satelital Sangolquí – Barrio San Jorge (Fuente: Cortesía de Googlemaps)

Gráfico: 6.11 Fotografía satelital de la ubicación del Centro Educativo La Pradera en Sangolquí (Fuente: Cortesía de googlemaps)

Número de Bloques a enlazar: 3

Gráfico: 6.12 Fotografía del Centro Educativo La Pradera (Fuente: cortesía de googlemaps)

Bloque 1: Latitud 0 grados 19’ 30.5”

Longitude: 78 grados 27´0.2 “

Bloque 2: Latitud: 0 grados 19’ 30.2”

Longitude 78 grados 26’ 58.7”

Bloque 3: Latitude 0 grados 19’ 29.6” S

Longitude 78 grados 27 ‘ 1.4 “ W

6.8.3.1.1 Servicios de red, protocolos y usuarios

Los servicios de red que requiere el CELP son: correo, mensajería interna, acceso al sistema de gestión, Internet

Los protocolos a utilizar son TCP/IP, Pop3, SMTP, 802.11b, Cifrado WPA2 para la red inalámbrica.

El número de usuarios de la red es 79 desglosados de la siguiente forma:

- Laboratorio Bloque 1: 15
- Bloque 2: 10
- Bloque 3: 6
- Red Inalámbrica: 40

- Servidores y dispositivos de comunicaciones: 8

6.8.3.1.2 Selección de Equipos

Para seleccionar los equipos se realiza un análisis de marcas, para lo cual se toma en cuenta los siguientes parámetros de evaluación:

Garantía:

No tiene garantía: 1; Limitada: 2; ilimitada 3

Consumo de energía: (Ver anexo 21)

Watts: de 1 a 23,1 - 5; 23,2 a 42,2 – 4 42,3 a 49,3 -3; 49,4 en adelante 2

Non-Poe: de 1 a 12.5 -5; 12,5 a 13 – 4; 13,1 a 14,5 – 3; 14,5 a 15,2 -2; 15,3 a 18,5-1

Rendimiento: (Ver anexo 21)

Marca	**Garantía**	**Costo**	**Consumo de energía Watts**		**Rendimiento**		**Calificación**
			Equipo	No-Poe	Throughput	Latencia	
CISCO	3	4	5	4	5	5	26
HP Networking	2	3	4	2	5	3	19
Dlink	2	5	3	3	3	2	18
Netgear	2	3	4	5	5	4	23

Tabla 6.22: Marcas de equipos de comunicaciones (Elaborado por: Investigador) (Fuente: (Reese, B., 2011, págs. 1-3)

La mejor marca por garantía, costo, consumo de energía, rendimiento es CISCO por lo que se opta por trabajar con esta marca para los equipos de comunicaciones.

Los equipos que se necesitan para el diseño de la Red Jerárquica son:

Cant.	Equipo	Marca	Descripción	P. unit	Total
2	switch	CISCO	Smart Switch FE de 24-Puertos 10/100 + 2 puertos (RJ-45 + SFP) combinados; 128 VLANs	224.79	449.58
3	switch	CISCO	Administrable capa 3 de 24 puertos 10/100/1000 + 2 puertos GigE + 2 1GE SFP combinados; 4092 Vlans	852.60	2557.80
2	router wireless	CISCO	Router wireless-N 5 VPN firewall; 4 puertos LAN 10/100 + 1 WAN 10/100; 2 antenas integradas; 32 Usuarios; 2.4 GHz	101.85	203.70
2	Access Point	CISCO	Access Point N 300 Mbps doble banda w/PoE + Portal Cautivo Hot Spot + Roaming Port 10/100/1000 cluster max 8 Aps	274.05	548.10
1	UPS	forza	Ups Forza Fx-2200 Lcd Ups Inteligente 120v Usb 2299 va (para los equipos de comunicaciones)	277.00	277.00
1	UPS	forza	Ups Forza Fx-2200 Lcd Ups Inteligente 120v Usb 2299 va /para los servidores)	277.00	277.00
					4313.18

Tabla 6.23: Lista de equipos para el diseño de la Red Jerárquica (Elaborado por: Investigador) (Fuente: Proforma anexo 16)

6.8.3.1.3 Selección de Servidores

Se considera dos servidores ya que el CELP (servidor proxy y otro para el servidor de autenticación para la red inalámbrica) ya que cuenta con un servidor de aplicaciones.

Cant.	Equipo	Marca	Descripción	P. UNIT	TOTAL
2	Servidor SERHPX675421001		HP DL320e Gen8 E3-1220v2 Hot Plug US Svr 1U Rack / Intel® Xeon™ Quad-Core E3-1220v2 (3.1GHz, 69W, 8MB) / 4GB (1 x 4GB) UDIMM / No incluye discos duros / HP Ethernet 1Gb 2-port 330i Adapter / HP Smart Array B120i/Zero Memory SATA (0/1/1+0) / 350W Non-hot plug Power Supply / 4 ventiladores Non-hot plug, Non-Redundant / HP iLO Management Engine / 1 año en piezas, mano de obra on site	1002	2004
2	Disco Duro X658071B21		HP 500GB 6G SATA 7.2k 3.5in SC MDL HDD	212	424
				TOTAL	**2428**

Tabla 6.24: Selección de servidores (Fuente: Cotización Espiral Sistemas- Anexo 18)

6.8.3.1.4 Selección de Materiales

Para la selección de materiales se tomó en cuenta que sean marcas reconocidas como Levinton, Beaucoup que ofrece garantía de por vida, Nitrotel, Schneider y Rymco que son marcas de renombre.

A continuación se presenta la tabla 6.25 donde se presenta la lista de los equipos de conectividad necesarios para la red.

Cant.	Equipo	Marca	Descripción	P. UNIT	TOTAL
1	Rack JTP-842430N	BEAUCOUP	Rack cerrado 79P. 2000x600x800MM negro puerta vidrio	931.90	931.90
1	Bandeja BNJ-101V	BEAUCOUP	Bandeja estándar 2Ur 19P 89.5x444x367mm ventilada (router)	17.10	17.10
1	Organizador vertical	BEAUCOUP	Organizador vertical simple 80x80 72	47.10	47.10
2	Organizador horizontal	BEAUCOUP	Organizador horizontal con canaleta 60x80 19P	15.43	30.86
1	Multitomas	LEVITON	Regleta cortapicos de 12 puertos para rack (para equipos de comunicación y servidores)	196.11	196.11
2	Patch Pannel	Nitrotel	Patch Panel Utp Cat6 24 Puertos 110idc T568 A/b Nitrotel	69.00	138.00
6	Rollos cable UTP	LEVITON	Cable Cat 5E CMR color azul, 255 m c/rollo	0.44	671
1	Cable de teléfono	Sin marca	Cable telefónico de 3 m	2.00	2.00
40	Face Plate	LEVITON	2 posiciones blanco	1.63	65.20
48	Patch cords	LEVITON	Patch cord cat 5E 3 pies blanco	2.16	103.68
48	Patch cords	LEVITON	Patch cord cat 5E 7 pies blanco	2.75	103.68
5	Cajas de Canaletas	Schneider Electric	Canaletas Plásticas Con Division Pvc 60x40 Mm (caja 10und) Canaleta Dexson - Schneider Electric Con División De 2 Mts	98.00	490.00
20	Tomas eléctricas	LEVITON	Tomacorriente doble polarizado comercial blanco	0.65	13.00
12	Tubo metálic	RYMCO	5m /1 pulgada	5.00	60.00
11	Uniones met	RYMCO	1 pulgada	1.00	11.00
					2880.63

Tabla 6.25: Equipos de conectividad (Elaborado por: Investigador) (Fuente: Proforma Anexo 17)

6.8.3.1.5 Selección de la topología de red

Tomando en consideración los problemas de la red encontrados como son: segmentos de red divididos, interfaces de red mal colocadas, configuración lógica de la red en el sistema operativo inadecuada, equipos de comunicaciones sin protección, equipos de comunicaciones desconectados, compartición del Internet por medio del switch de un segmento, compartición del Internet con squid sin configurar seguridades de otro segmento, acceso restringido para encender los equipos de comunicaciones, tubería de cableado telefónico mojada, cableado telefónico roto, problemas con proveedor de Internet, falta de gestión en red, conflictos de direcciones IP en la red inalámbrica; tiempo respuesta para acceso al sistema de gestión de la información que funciona en red extremadamente lento; se prevee la creación de un laboratorio en el Bloque 2 en cuanto a equipos de comunicaciones para que funcione como centro de capacitaciones en las tardes y se establece la realización de un modelo de red jerárquico.

Las red jerárquica ayuda a hacerle más predecible, entendible, a aplicar la configuración más adecuada; y podrá ser administrado con un manual de usuario por la persona encargada de tecnología a futuro; las ventajas son el escalamiento, facilidad de diseño, implementación, confiabilidad. En el gráfico 6.13 y 6.14 se puede observar el diseño de la Topología Física de la Red.

En donde se puede observar la presencia de tres capas la capa de núcleo, la capa de distribución, la capa de acceso.

En la capa de núcleo se encuentra un router capa 3 con los servidores a utilizar, en la capa de distribución se encuentran 3 switches, uno para cada bloque conectados entre si, y en la capa de acceso se encuentran los switches para cada área, interafaces de red, 2 routers inalámbricos para 2 redes inalámbricas para el área administrativa y para uso de los docentes en las aulas.

6.8.3.1.6 Topología Física

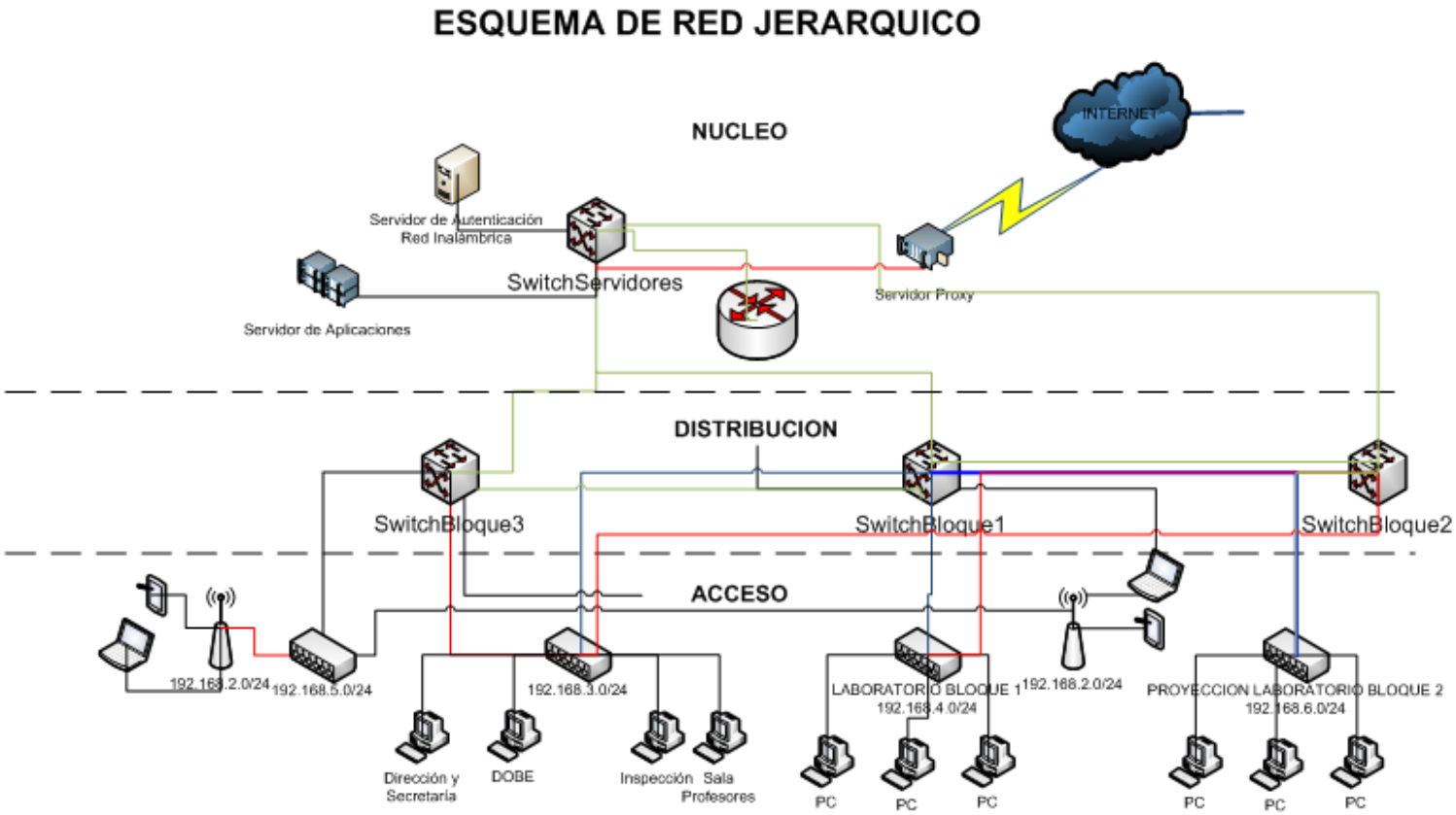


Gráfico: 6.13 Esquema de Red Jerárquico propuesto (Elaborado por: Investigador)

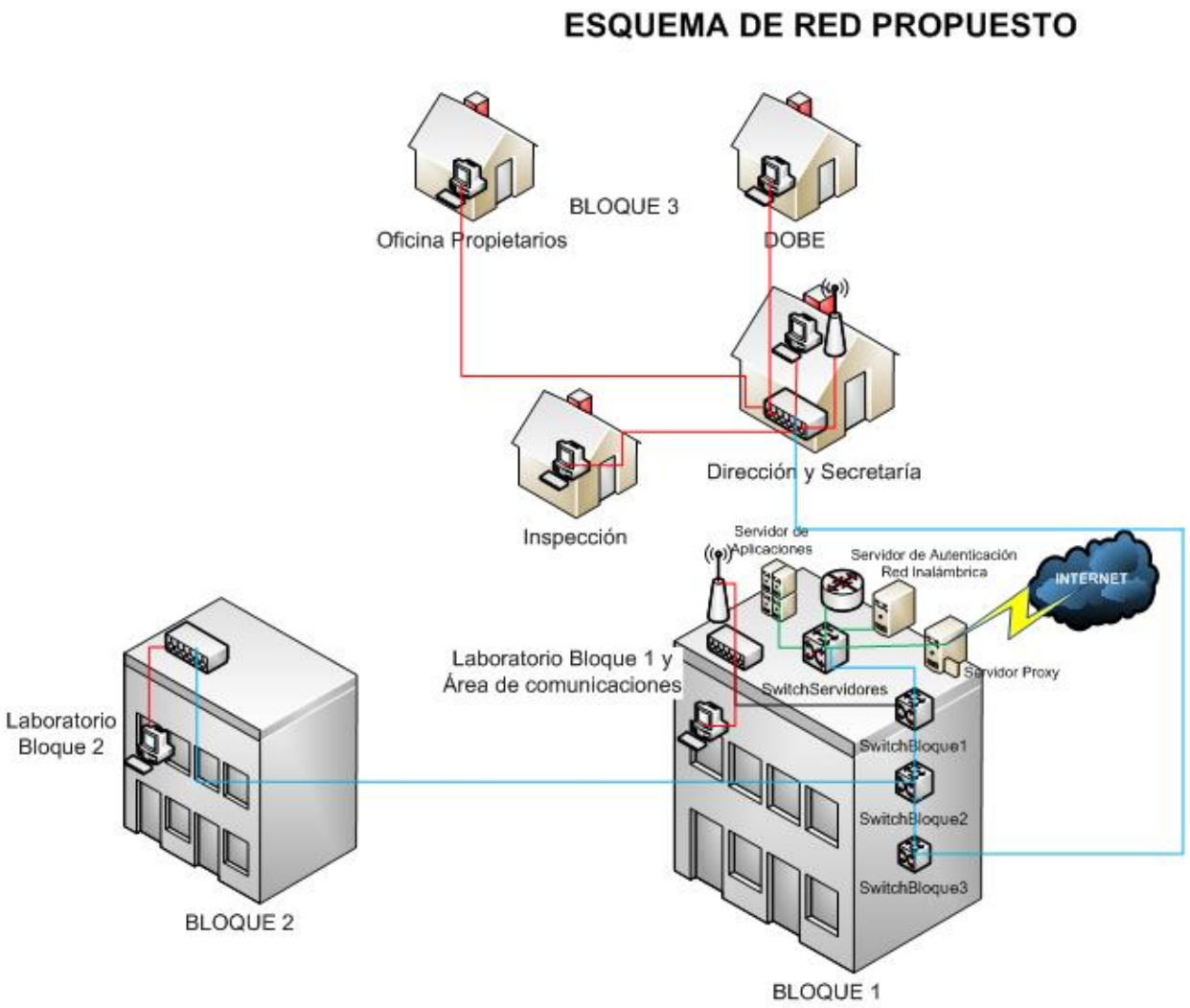


Gráfico: 6.14 Esquema de red Propuesto (Elaborado por: Investigador)

6.8.3.1.7 Tabla de Direccionamiento Bloque 1

La tabla de direccionamiento indica la dirección IP con la sub-máscara de red para cada interface de los equipos.

Direccionamiento				
Bloque 1		**Equipos**	**Ips**	**Máscara**
Laboratorio Bloque 1: 192.168.4.0	Cuarto de comunica-ciones	Servidor Proxy - firewall	192.168.6.100	255.255.255.0
		Switch Capa 3 - Bloque 1	192.168.6.101	255.255.255.0
		Switch Capa 3 - Bloque 3	192.168.6.102	255.255.255.0
		Switch Capa 3 - Servidores	192.168.6.103	255.255.255.0
		Router Wireless Administrativo	192.168.6.104	255.255.255.0
		Router Wireless Laboratorio	192.168.6.105	255.255.255.0
		Servidor de Aplicaciones	192.168.6.106	255.255.255.0
		Servidor de autenticación red inalámbrica	192.168.6.107	255.255.255.0
	Estudiantes	LAB_B1_01	192.168.4.1	255.255.255.0
		LAB_B1_02	192.168.4.2	255.255.255.0
		LAB_B1_03	192.168.4.3	255.255.255.0
		LAB_B1_04	192.168.4.4	255.255.255.0
		LAB_B1_05	192.168.4.5	255.255.255.0
		LAB_B1_06	192.168.4.6	255.255.255.0
		LAB_B1_07	192.168.4.7	255.255.255.0
		LAB_B1_08	192.168.4.8	255.255.255.0
		LAB_B1_09	192.168.4.9	255.255.255.0
		LAB_B1_10	192.168.4.10	255.255.255.0
		LAB_B1_11	192.168.4.11	255.255.255.0
		LAB_B1_12	192.168.4.12	255.255.255.0
		LAB_B1_13	192.168.4.13	255.255.255.0
		LAB_B1_14	192.168.4.14	255.255.255.0
		LAB_B1_15	192.168.4.15	255.255.255.0

Tabla 6.26: Tabla de Direccionamiento Bloque 1 (Elaborado por: Investigador)

6.8.3.1.8 Tabla de Direccionamiento Bloque 2

Bloque 2		Equipos	Ips	Máscara
Proyección Laboratorio Bloque 2 192.168.5.0	Estudiantes	LAB_B2_01	192.168.5.1	255.255.255.0
		LAB_B2_02	192.168.5.2	255.255.255.0
		LAB_B2_03	192.168.5.3	255.255.255.0
		LAB_B2_04	192.168.5.4	255.255.255.0
		LAB_B2_05	192.168.5.5	255.255.255.0
		LAB_B2_06	192.168.5.6	255.255.255.0
		LAB_B2_07	192.168.5.7	255.255.255.0
		LAB_B2_08	192.168.5.8	255.255.255.0
		LAB_B2_09	192.168.5.9	255.255.255.0
		LAB_B2_10	192.168.5.10	255.255.255.0

Tabla 6.27: Tabla de Direccionamiento Bloque 2 (Elaborado por: Investigador)

6.8.3.1.9 Tabla de Direccionamiento Bloque 3

Bloque 3		Equipos	Direccionamiento	Máscara
		Secretaría	192.168.3.2	255.255.255.0
		DOBE	192.168.3.3	255.255.255.0
		Inspección	192.168.3.4 - 192.168.3.8	255.255.255.0
		Dirección	192.168.3.9	255.255.255.0
		Sala de Docentes	192.168.3.10 - 192.168.3.16	255.255.255.0
		Propietarios	192.168.3.17	255.255.255.0
Red Inalámbrica: 192.168.2.0	Invitados	Invitados, Docentes-Autoridades	192.168.2.1 - 192.168.2.40	255.255.255.0

Tabla 6.28: Tabla de Direccionamiento Bloque 3 (Elaborado por: Investigador)

6.8.4 Plan de capacitación al Personal Docente

Fecha Ini: 15-03-2014	**Fecha Fin:** 7-05-2014	**Hora:** 14h00-15h00	**Lugar:** Laboratorio de Tics	**Núm. Horas:** 40
Objetivo: Aprender a usar herramientas guiadas como webquest y caza de tesoro para mejorar la seguridad informática en el uso de Tics en el Centro Educativo La Pradera				
Necesidad: Seguridad Informática usando Tics.		**Método:** Inductivo – deductivo	**Instructor**: Ing. Tannia Mayorga	

Temática	Horas	Destreza	Recursos
1. Tics Introducción a las Tics La alfabetización digital Integración y uso de las Tics en la educ. Historia	2	Conocer la Evolución del uso de las tecnologías en la educación con sus ventajas.	**Recursos audiovisuales:** -Proyector **Equipos** -Computador para instructor - 15 computadores **Herramientas** - Internet -Prezzy -Webquest creator -Internet **Manuales** -Webquest creator
2. Evaluación y selección de software de recursos educativos	2	Tener criterio para la selección de recursos tecnológicos a ser utilizado en el aula.	
3. Técnica de aprendizaje con Tic	1	Saber cuándo aplicar las Tics como técnica de aprendizaje en el aula.	

Tabla 6.29: Plan de capacitación al Personal Docente sobre Herramientas guiadas (Elaborado por: Investigador) (cont.)

Tabla 6.29: Plan de capacitación al Personal Docente sobre Herramientas guiadas (cont.)

Fecha Ini: 15-03-2014	**Fecha Fin:** 7-05-2014	**Hora:** 14h00-15h00	**Lugar:** Laboratorio de Tics	**Núm. Horas:** 40
Objetivo: Aprender a usar herramientas guiadas como webquest y caza de tesoro para mejorar la seguridad informática en el uso de Tics en el Centro Educativo La Pradera				
Necesidad: Seguridad Informática usando Tics.		**Método:** Inductivo – deductivo	**Instructor**: Ing. Tannia Mayorga	

Temática	**Horas**	**Destreza**	**Recursos**
4. Internet ¿Qué es? Servicios de Internet Acceso a la información	3	Conocer los servicios que ofrece el Internet y que pueden ser usados en el aula	…
5. Evaluación del material de aprendizaje	1	Evaluar el material de aprendizaje a ser utilizado en el aula	
6. Internet como herramienta de apoyo en el aula Introducción Aspectos a tomar en cuenta	2	Ver como se puede usar el Internet como herramienta de apoyo en el aula	

Tabla 6.29: Plan de capacitación al Personal Docente sobre Herramientas guiadas (Elaborado por: Investigador) (cont.)

Tabla 6.29: Plan de capacitación al Personal Docente sobre Herramientas guiadas (cont.)

Fecha Ini: 15-03-2014	**Fecha Fin:** 7-05-2014	**Hora:** 14h00-15h00	**Lugar:** Laboratorio de Tics	**Núm. Horas:** 40
Objetivo: Aprender a usar herramientas guiadas como webquest y caza de tesoro para mejorar la seguridad informática en el uso de Tics en el Centro Educativo La Pradera.				
Necesidad: Seguridad Informática usando Tics.		**Método:** Inductivo – deductivo	**Instructor**: Ing. Tannia Mayorga	

Temática	**Horas**	**Destreza**	**Recursos**
Web 2.0 y 3.0 Uso de la web en la clase Webquest Caza del Tesoro o búsqueda del tesoro	6	Usar la web 2.0 y 3.0 para sacar material para ser usado cuando se elabore las webquests y cazas de tesoro	…
7. Las webquest -introducción. Estructura Ejercicio	6	Hacer su primera webquest	
8. Caza de Tesoro Definición Estructura Ejercicio	6	Hacer su primera Caza de tesoro	

Tabla 6.29: Plan de capacitación al Personal Docente sobre Herramientas guiadas (Elaborado por: Investigador) (cont.)

Tabla 6.29: Plan de capacitación al Personal Docente sobre Herramientas guiadas (cont.)

Fecha Ini: 15-02-2014	**Fecha Fin:** 7-04-2014	**Hora:** 14h00-15h00	**Lugar:** Laboratorio de Tics	**Núm. Horas:** 40
Objetivo: Aprender a usar herramientas guiadas como webquest y caza de tesoro para mejorar la seguridad informática en el uso de Tics en el Centro Educativo La Pradera.				
Necesidad: Seguridad Informática usando Tics.		**Método:** Inductivo – deductivo	**Instructor**: Ing. Tannia Mayorga	

Temática	**Horas**	**Destreza**	**Recursos**
9. Herramientas de creación de webquest Webquestcreator	5	Conocer varias herramientas donde hacer webquests y cazas de tesoro	…
10. Exposición de trabajo final	7	Presentar al grupo el trabajo de fin de curso aplicando todos los conocimientos	
TOTAL	**40**		

- **Personal a ser capacitado:** Personal Docente — **Número de Personas:** 15
- **Grado de habilidad:** Manejo del computador — **Tiempo y periodicidad:** 1 hora por 40 días
- **Características personales:** Ganas de aprender — **Costo:** Tiempo
- **Relación costo beneficio:** Durante las clases, los profesores podrán hacer uso de las Tics en el aula e incluirla en el currículo en forma segura, así la Institución podrá ganar calidad y prestigio tecnológico; y los estudiantes del CELP se verán beneficiados en el aprendizaje utilizando el Internet como herramienta de apoyo en su formación.

Tabla 6.29: Planificación de la capacitación sobre Herramientas guiadas: Webquest y Caza de Tesoro al personal docente
(Elaborado por: Investigador)

6.8.5 Plan de Taller para padres de familia sobre seguridad informática

Fecha: 15-03-2014	**Hora:** 17h00-19h30	**Núm. Horas:** 2h30	**Lugar:** Auditorio CELP	**Núm. participantes:** 190
Objetivo: Dar a conocer los peligros y beneficios del Internet como herramienta de formación para los niños, niñas y adolescentes del CELP.				
Necesidad: Seguridad Informática en el CELP.	**Método:** Técnicas Grupales	**Instructor**: Ing. Tannia Mayorga		

Temática		Recursos
Presentación	5’	**Recursos audiovisuales:**
Expectativas del Taller	10’	-Proyector
Seguridad informática Introducción Ventajas	10’	**Equipos** -Computador para instructor **Herramientas**
Trabajo grupal (1ra parte) Ejercicio de roles (Padres – Hijos), temática **desventajas** del uso de Internet. Sensibilización del ejercicio en el grupo Socialización por grupo de lo que aprendieron de la experiencia (un representante)	60´	- Internet - Prezzy **Materiales** -Papelote -Marcadores **Manuales** -Guía resumen del Taller

Tabla 6.30: Estructura del Taller de Padres de Familia sobre seguridad informática (Elaborado por: Investigador) (cont.)

Tabla 6.30: Estructura del Taller de Padres de Familia sobre seguridad informática (cont.)

Fecha: 15-03-2014	**Hora:** 17h00-19h30	**Núm. Horas:** 2h30	**Lugar:** Auditorio CELP	**Núm. participantes:** 190
Objetivo: Dar a conocer los peligros y beneficios del Internet como herramienta de formación para los niños, niñas y adolescentes del CELP.				
Necesidad: Seguridad Informática en el CELP.	**Método:** Técnicas Grupales	**Instructor**: Ing. Tannia Mayorga		
Temática			**Min.**	**Recursos**
Trabajo grupal (2da parte) Amenazas y vulnerabilidades Explicación Socialización del ejercicio en el grupo Exposición de un representante del grupo			 5’ 15’	…
Soluciones Tecnológicas A nivel de software A nivel de hardware			30´	
Evaluación del Taller			5´	
Cierre			10´	
Grado de habilidad, conocimientos y actitudes: Dirigida para cualquier público **Características personales:** Ganas de aprender en pro de mejorar la seguridad de sus hijos(as) **Relación costo beneficio:** Conciencia del uso de Internet para la formación de los niños, niñas y adolescentes				

Tabla 6. 30: Estructura del Taller de Padres de Familia sobre seguridad informática (Elaborado por: investigador)

6.9 Administración

- Encargado de Tecnología
  Ing. Byron Bravo
- Director - Propietario
  Arq. Luis Atapuma
- Profesor de Tics
  Lic. David De La Cruz
- Secretaria
  Lic. Cecilia Rodríguez
- Inspectora
  Lic. Viviana Sanguano

6.10 Plan de Acción

Id	Nombre de tarea	Duración	Comienzo	Fin
1	**Fase 1 Establecer Plan de seguridad informática**	**78 días**	**mar 30/07/13**	**vie 15/11/13**
2	Definir objetivos, importancia	2 días	mar 30/07/13	mié 31/07/13
3	Definir alcance y límites	5 días	jue 01/08/13	mié 07/08/13
4	Definir marco referencial	30 días	jue 08/08/13	mié 18/09/13
5	Estimación del riesgo	15 días	jue 19/09/13	mié 09/10/13
6	Tratamiento de riesgo	2 días	jue 10/10/13	vie 11/10/13
7	Enunciado de aplicabilidad	3 días	lun 14/10/13	mié 16/10/13
8	Definir documentación del plan	22 días	jue 17/10/13	vie 15/11/13
9	**Fase 2 Diseño de la Red**	**21 días?**	**jue 08/08/13**	**jue 05/09/13**
10	Análisis de requerimientos	4 días	jue 08/08/13	mar 13/08/13
11	Selección de equipos y materiales	10 días?	mié 14/08/13	mar 27/08/13
12	Topología de Red	4 días	mié 28/08/13	lun 02/09/13
13	Establecer el direccionamiento adecuado	3 días	mar 03/09/13	jue 05/09/13
14	**Fase 3 Establecer Plan de Capacitación al Personal Docente**	**18 días**	**vie 06/09/13**	**mar 01/10/13**
15	Determinar temas a tratar	3 días	vie 06/09/13	mar 10/09/13
16	Armar el plan de capacitación	15 días	mié 11/09/13	mar 01/10/13
17	**Fase 4 Establecer Plan del Taller de Padres de Familia**	**12 días**	**mar 12/11/13**	**mié 27/11/13**
18	Identificar necesidades de seguridad	2 días	mar 12/11/13	mié 13/11/13
19	Definir estructura de capacitación	10 días	jue 14/11/13	mié 27/11/13
20	**Fase 6 Entrega de la Propuesta al Propietario del Centro Educativo "La Pradera"**	**3 días**	**jue 28/11/13**	**lun 02/12/13**
21	Evaluación de la propuesta	3 días	jue 28/11/13	lun 02/12/13

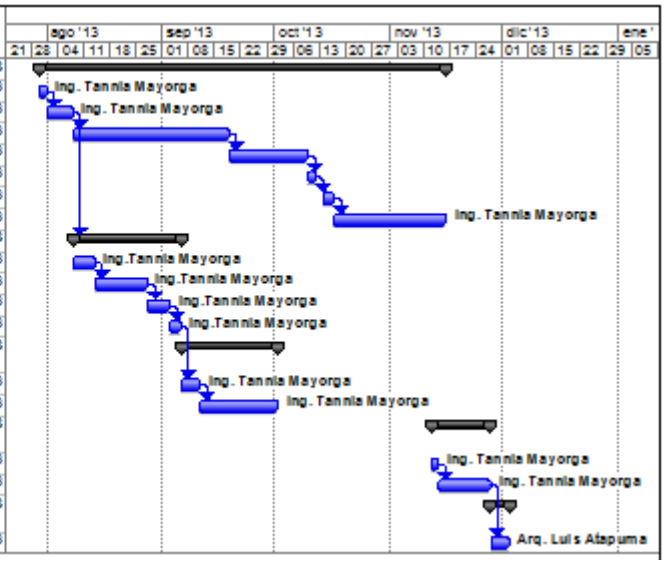


Gráfico: 6.15 Plan de Acción para la Propuesta (Elaborado por: Investigador)

6.11 Previsión de la Evaluación

Para la evaluación estarán presentes:

Nombre	Cargo
Arq. Luis Atapuma	Propietario - Director
Sra. Zoila Días de Atapuma	Propietaria
Lic. David De La Cruz	Profesor de Tics
Lic. Viviana Sanguano	Jefe de Talento Humano
Lic. Cecilia Rodríguez	Secretaria

6.12 Evaluación

6.12.1 Gráficas de la encuesta realizada sobre la evaluación de la Propuesta

Luego de la presentación se aplicó la encuesta dirigida a los propietarios y jefaturas.

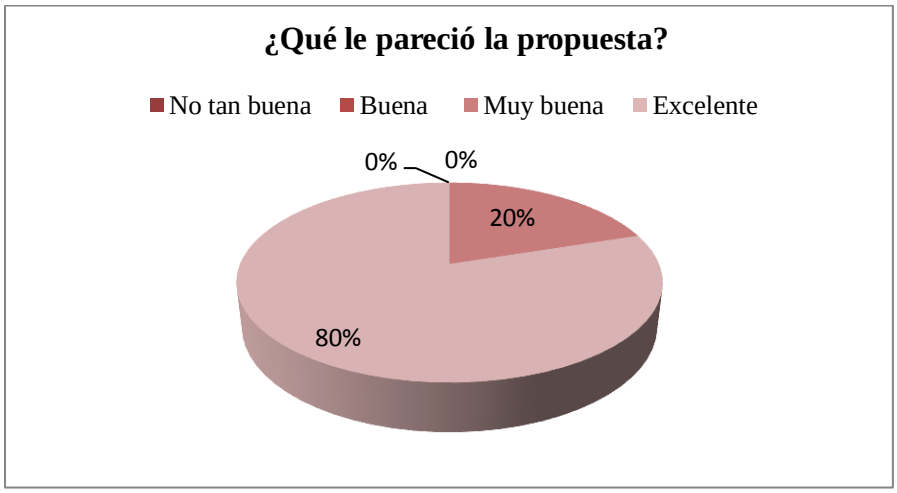


Gráfico: 6.16 Evaluación de la propuesta por parte de los propietarios y jefaturas (Elaborado por: Investigador)

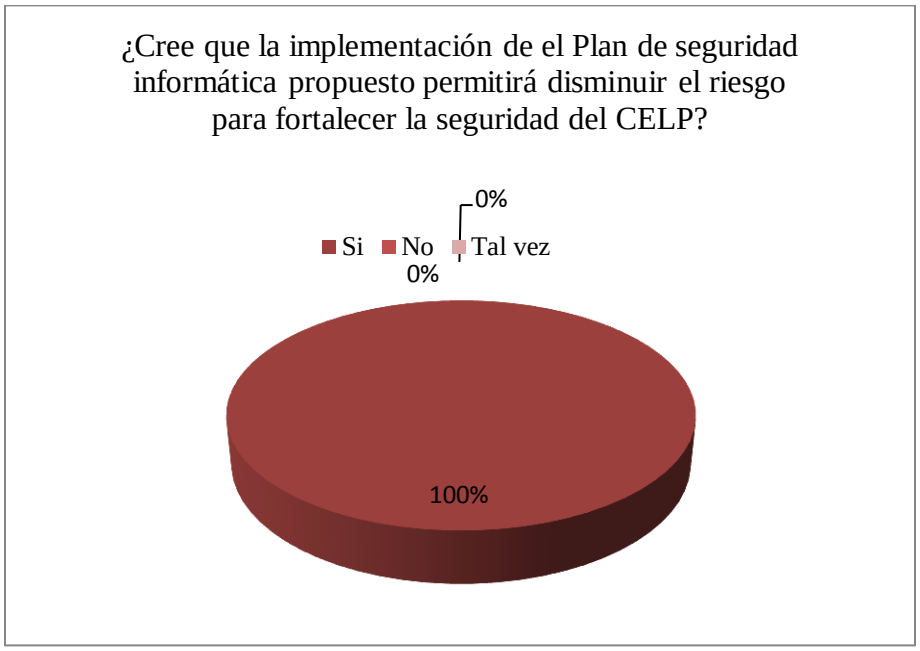


Gráfico: 6. 17 Evaluación del Plan de seguridad informática la Propuesta (Elaborado por: Investigador)

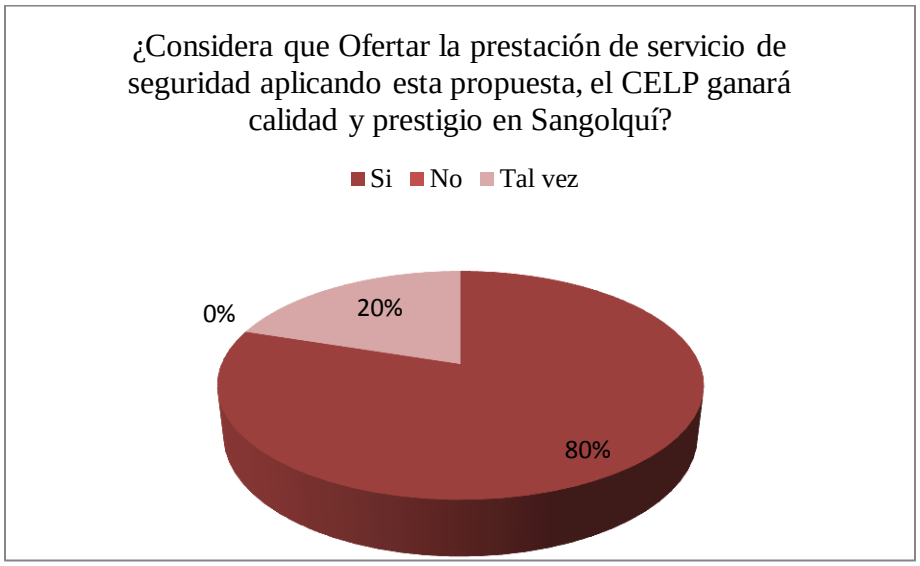


Gráfico: 6.18 Evaluación Plan de seguridad informática referente a oferta de la prestación se servicio de seguridad para ganar calidad y prestigio (Elaborado por: Investigador)

6.12.2 Evaluación sobre los resultados de la propuesta mediante una entrevista a los padres de familia.

Pregunta	Respuesta 1	Respuesta 2	Respuesta 3
¿Cree usted que aplicar estándares ISO 27001 mediante un Plan de seguridad informática ayudaría al Centro Educativo La Pradera a fortalecer la seguridad de los estudiantes?	Si	Sería bueno ya que las instituciones serias lo aplican	Por supuesto
¿Le gustaría conocer sobre los Peligros del uso de Internet en los niños, niñas y adolescentes?	Si para prevenir esas cosas	Si ya que los Padres necesitamos ponernos al día	Si, la pornografía está de moda
¿Le gustaría conocer sobre las ventajas de usar el Internet como herramienta de apoyo en la formación de sus hijos(as)?	Siempre es bueno aprender	Si	Si
Le interesaría saber ¿cuáles herramientas se pueden usar para poner seguridades informáticas en casa?	Si	Sería bueno	Si hay como ayudarles desde la casa
¿Qué le parece que el CELP", dicte un Taller sobre Seguridad informática para padres de familia con el objetivo de ayudar a mejorar la seguridad integral de sus hijos(as)?	Excelente	Muy bueno, ojalá que nos ayuden a los Padres de esa forma	Buenísimo
¿Le gustaría que el personal docente se capacite en el uso de herramientas de Internet para ayudar a mejorar la formación de sus hijos de una manera segura?	Si	Si	Si

Tabla 6.31: Entrevista dirigida a los padres de familia sobre la Propuesta (Elaborado por: Investigador)

6.12.3 Evaluación del Investigador configurando el proxy utilizando squid con seguridades a nivel de software durante la clase de Sociales

Se montó un squid en el Laboratorio de Tics del Bloque 1, previa la presentación de esta propuesta y se midió la clase de Sociales con la Docente Johana Tapia, tutora de séptimo año de educación básica utilizando seguridad a nivel de software, en la que el 100% de los estudiantes, incluida la Docente accedieron únicamente a las páginas pertinentes, hubo intentos de acceso por parte de los estudiantes, que fueron bloqueados por dicho software como se puede ver en la siguiente gráfica.

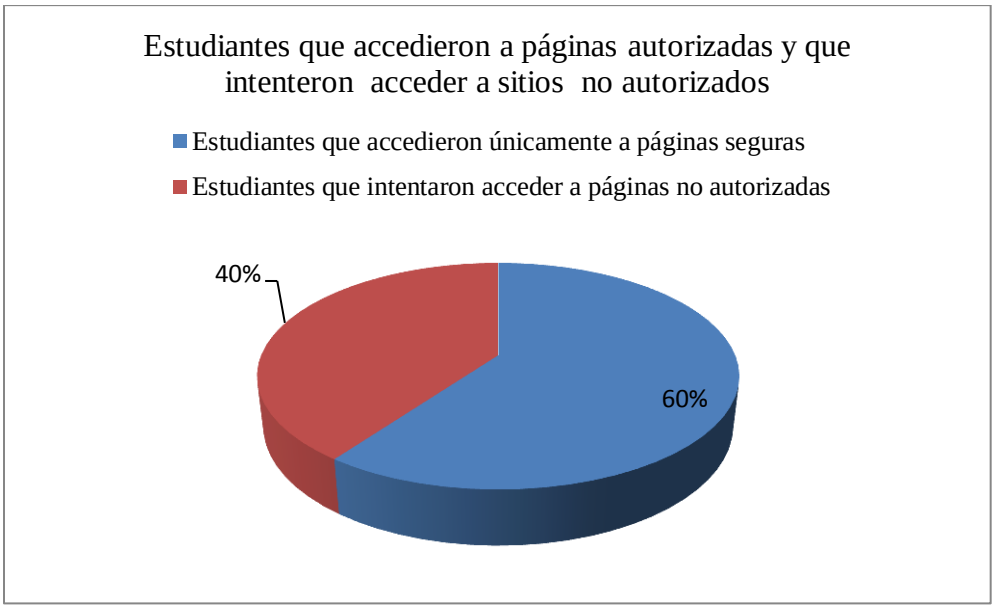


Gráfico: 6.19 Estudiantes con intentos de acceso no autorizado luego de aplicar seguridad usando software squid durante la clase de Sociales (Elaborado por: Ivestigador)

6.13 Conclusiones y Recomendaciones de la Propuesta

6.13.1 Conclusiones

- El Plan se seguridad informática, junto con el Plan de capacitación a docentes y padres de familia ayudará a mejorar la seguridad de la información del CELP y podrá servir de base para que otras entidades educativas sigan este modelo.
- La norma ISO 27001:2005, ISO 27002: 2005, ISO 27005:2008 son normas muy valiosas ya que tienen los pasos para implementar un Sistema de Gestión de Seguridad de la información, establecer controles, hacer el análisis de riesgos de cualquier institución y el éxito de su aplicabilidad está en realizar continuamente revisiones de la seguridad definiendo a un responsable de velar que esto se cumpla con el apoyo de Gerencia o Dirección, Consejos ejecutivos para el caso de las entidades educativas.
- Un sistema de gestión de seguridad de la información tiene que ser tomado con mucha seriedad y debe ser apoyado, realizado con la participación de las jefaturas, autoridades, propietarios y todos los involucrados en la seguridad informática sin olvidar que una vez implementado es fundamental que se de un seguimiento para prevenir futuros riesgos.
- Para que las políticas de seguridad informática estén bien elaboradas es necesario que previo a ello se realice un análisis de riesgos y se de el tratamiento de riesgos apropiado con la finalidad de prevenir amenazas.
- Es una gran responsabilidad estar al frente de la elaboración de un Sistema de Gestión de Seguridad de la Información ya que requiere de involucrarse en los procesos de negocio de la Institución, donde se va a trabajar, al igual que tener conocimiento, experiencia en las áreas de tecnología donde se va a realizar el análisis de riesgos para ir encontrando las vulnerabilidades, o ir identificando las amenazas.

6.13.2 Recomendaciones

- Evaluar continuamente el plan de seguridad informática. hacer un seguimiento adecuado del cumplimiento de las seguridades establecidas, capacitar continuamente sobre seguridad informática tanto a estudiantes, docentes como a padres de familia.
- Para el próximo año se recomienda aplicar los nuevos controles recomendados en la norma ISO 27001:2013, ISO 27002:2013 que fue publicada el 14 de octubre del 2013, cabe señalar que se podrá aplicar la ISO 27001:2005 un año más y para el próximo se recomienda actualizarse a la nueva versión.
- Es necesario incluir en un futuro Plan SGSI el Sistema de Gestión de Información (no se analizó a detalle porque estaban en proceso de desarrollo y no se encontraba implementado) al igual que la página web que va a estar integrada con el sistema ya que se encontraron algunas vulnerabilidades, y por ende están sujetas a amenazas.
- El cumplimiento con requerimientos legales en lo referente a licenciamiento, es necesario que sea tomado en cuenta a futuro ya que es una vulnerabilidad que fue tratada en el análisis de riesgo y la decisión fue "mantener el riesgo".

MATERIALES DE REFERENCIA

Trabajos Citados

Reglamento a la Ley Orgánica de Educación Intercultural. (31 de 03 de 2011). 109. Quito, Ecuador: Suplento registro oficial 417.

Aguilera, P. (s.f.). *Seguridad Informática.* (G. Morlanes, Ed.) Madrid, España: Editex.

Alegsa. (2012). *Diccionario de informática*. Recuperado el 22 de 06 de 2013, de http://www.alegsa.com.ar/Dic/seguridad%20informatica.php

Barroso, O. (2004). *La red como instrumento de búsqueda de información y comunicación.* Granada.

Bautista, L. (2013). *Plan de Seguridad de la Información.* España: Universitat Oberta de Catalunya. Recuperado el 9 de nov de 2013, de http://hdl.handle.net/10609/19443

Campusano Rodríguez, R. (2011). *Estudio, propuesta y aplicación de políticas de seguridad en los laboratorios de informática en las instituciones educativas de nivel básico.* Cuenca, Azuay, Ecuador: Universidad Tecnológica Israel.

Castells, M. (2010). *Sociedad Red* (Segunda ed.). Barcelona, España: UOC.

Chamorro, V. (2013). *Plan de Seguridad de la Información basado en el estandar ISO 13335 aplicado a un caso de estudio.* Quito, Pichincha, Ecuador: Escuela Politécnica Nacional.

Clayton, J. (2002). *Diccionario Ilustrado de telecomunicaciones.* McGraw-Hill.

Definición ABC. (2007). *Definición ABC*. Recuperado el 6 de 10 de 2013, de http://www.definicionabc.com/general/herramienta.php

Departamento de obras de referencia Ediciones Trébol,S.L. (2007). *Diccionario Enciclopédico.* Lima, Barcelona, España: Trébol, S.L.

Diario Hoy. (29 de abr de 2012). Menores expuestos a 7 amenazas en Internet. *Diario Hoy*.

Ecured. (27 de 10 de 2011). *http://www.ecured.cu/index.php/Telecomunicaciones*. Recuperado el 25 de 09 de 2013, de ecured.cu: http://www.ecured.cu/index.php/Telecomunicaciones

España, M. d. (12 de Feb de 2011). *Observatorio Tecnológico*. Recuperado el 2 de jun de 2013, de http://recursostic.educacion.es/observatorio/web/ca/cajon-de-sastre/38-cajon-de-sastre/961-monografico-redes-wifi?start=7

Gabavenda. (10 de nov de 2010). *La Teoría del bit*. Recuperado el 30 de jun de 2013, de http://lateoriadelbit.wordpress.com/2010/11/10/politica-de-seguridad-%E2%80%9Cmito-vs-realidad%E2%80%9D/

García, A., Huratado, C., & Alegre Ramos, P. (2011). *Seguridad Informática* (Primera ed.). Madrid, España: Paraninfo.

García, A., Hurtado, C., & Allegre, M. (2011). *Seguridad Informática* (Primera ed.). Madrid, España: Paraninfo.

Gobierno de Argentina. (11 de 2009). *ICIC Internet Sano.* Recuperado el 23 de 06 de 2013, de Programa nacional de infraestructuras críticas de información y ciberseguridad: http://www.internetsano.gob.ar/archivos/recomendaciones_navegacion_segura.pdf

Gobierno de la República del Ecuador. (2012). *Ley Orgánica de Educación Intercultural.* Quito, Ecuador.

Gobierno del Ecuador. (17 de 04 de 2002). Ley de Comercio Electrónico Firmas y Mensajes de Datos. (R. O. 557, Ed.) Quito, Pichincha, Ecuador. Recuperado el 6 de sep de 2013, de http://www.wipo.int/wipolex/en/text.jsp?file_id=243546

Gómez, Á. (2007). *Enciclopedia de la seguridad informática.* Alfaomega Grupo Editor.

Gómez, V. (2010). *Seguridad informática: básico.* Madrid: Starbook.

Goncalves, M. (2001). *Manual de firewalls.* McGraw-Hill.

Guazmayan, C. (2004). *El Internet y la investigación científica: el uso de los medios y las nuevas tecnologías en la educación.* Coop. Editorial Magisterio.

Gutierrez, J., & Tena, J. (s.f.). *Protocolos Criptográficos y Seguridad en Redes.* Universidad de Cantabria.

IEC/ITC 27005. (2008). *Normas ISO 27005.* Inglaterra.

IEC/ITC ISO 27001. (2005). *ISO 27001.* Inglaterra.

IETF. (sep de 1997). *The Internet Engineering Task Force (IETF).* Recuperado el 14 de jun de 2013, de http://www.ietf.org/rfc/rfc2196.txt: http://www.ietf.org/

ISO/ICE, ITC. (2005). *Normas ISO 27001.*

ISO/IEC. (13335-1:2004). ISO 13335-1.

ISO/IEC. (17799:2005).

ISO/IEC. (TR 18044:2004). *ISO 18044.*

Jaramillo, P. (20 de 08 de 2009). *SERENDIPITIC.* Recuperado el 7 de 10 de 2013, de http://ticserendipity.wordpress.com/2009/08/20/el-concepto-de-educacion/

Junta de Castilla y León - Consejería de Educación. (10 de 11 de 2013). *www.educa.jcyl.es*. Obtenido de http://www.educa.jcyl.es/ciberacoso/es/guias-informativas/guia-profesorado-centros-escolares

Larousse. (2009). Diccionario enciclopédico de la Lengua española. Larousse.

Lozano, J. (11 de 2008). *Investigación Exploratoria*. Recuperado el 30 de 06 de 2013, de http://janeth-investigacioniv.blogspot.com/2008/11/investigacion-exploratoria.html

Marañon, G. A. (2004). *Seguridad informática para empresas y particulares: el libro más completo y comprensible de seguridad informática para la empresa con aplicaicones, procedimientos y ejemplos prácticos para tomar decisiones relativas a la seguridad.* McGraw Hill Interamericana.

Matilla, A. (04 de 2013). *Blog de Seguridad Informática - Clase 1*. Recuperado el 22 de 06 de 2013, de http://www.agustinmantilla.com/clase-1-definicion-de-seguridad-informatica.html

Ministerio de Educación de Ecuador. (2013). *Educación básica*. Recuperado el 29 de jun de 2013, de http://educacion.gob.ec/educacion-general-basica/

Ministerio de Educación del Ecuador. (2013). *Educación Inicial*. Recuperado el 29 de jun de 2013, de Educación Inicial: http://educacion.gob.ec/educacion-inicial/

Ministerio de Inclusión Económica y Social. (09 de 2012). *Agenda para la igualdad de niños, niñas y adolescentes*. Recuperado el 22 de nov de 2013, de http://www.inclusion.gob.ec/wp-content/uploads/downloads/2012/09/master-agenda-ni%C3%B1ez-2da-edicion.pdf

Omerella, M. (s.f.). Recuperado el 29 de 09 de 2013, de http://www.iso27000.es/download/seguridad%20informaticavsinformacion.pdf

Ormella Meyer, C., & Asociados. (s.f.). ¿Seguridad informática vs. Seguridad de la información?

Patrick , D. (2003). *The Security Policy Life Cycle: Functions and Responsibilities.* Edited by Tipton & Krause, .

Pellejo, I., Andreu, F., & Lesta, A. (2006). *Fundamentos y aplicaciones de Seguridad en redes WLAN.* Barcelona: MARCOBO.

Poveda, J.M. (mar de 2011). *Los activos de seguridad de la información.* Recuperado el 27 de 10 de 2013, de Wordpress.com: http://jmpovedar.files.wordpress.com/2011/03/mc3b3dulo-7.pdf

Prudencio Aguado, D. (2012). *Seguridad Informática para el Hogar.* España: Bubok Pblishing S. L.

Pujadas I Jubany, J. (2008). *Seguridad Informática en Centros Educativos de Valladolid.* Valladolid. Recuperado el 8 de Junio de 2013, de http://www.bellera.cat/josep/pfsense/Valladolid-2008-07-03_v12.pdf

Quantum Ignis. (01 de 11 de 2013). *Quantum Ignis*. Recuperado el 23 de nov de 2013, de http://quantumignis.jimdo.com/articulos-t%C3%A9cnicos/incendios-de-origen-electrico/

Reese, B. (25 de 2 de 2011). *www.badreese.com.* Obtenido de http://www.bradreese.com/blog/2-25-2011.htm

Rodao, J. d. (2002). *Piratas cibernéticos: ciberwars, seguridad informática e internet* (2002 ed.). Alfaomega.

Rodriguez, D. M. (2002). *Sistemas Inalambricos de Comunicacion Personal.* Mexico: ALFAOMEGA.

RomeroTerreno, M. d., Barbancho Concejero, J., Berjumea Modejar, J., Rivera Romero, O., & Ropero Rodriguez, J. (2010). *Redes Locales* . Madrid: Parainfo,SA.

Rosique, R. (s.f.). *www.academia.edu.* Recuperado el 1 de 11 de 2013, de http://s3.amazonaws.com/academia.edu.documents/31001786/Un_asomo_a_la_Educacion_y_Web_1.pdf?AWSAccessKeyId=AKIAJ56TQJRTWSMTNPEA&Expires=1389028455&Signature=99FaoGCw2a%2Ba1OrAAv1nJQCnHhw%3D&response-content-disposition=inline

Segura, J. (2005). Internet en el aula las WebQuest. *Revista electrónica tecnológica educativa*(17).

Tewari, A. (6 de 2 de 2013). *www.sisainfosec.com.* Recuperado el 7 de 10 de 2013, de http://sisainfosec.com/blog/comparison-between-iso-27005-octave-nist-sp-800-30-2/

UNESCO. (2010). unesco. *Conclusiones de TICs en la Educación.* Recuperado el 1 de junio de 2013, de Unesco: http://unesdoc.unesco.org/images/0019/001905/190555s.pdf

Universidad de Jaén. (2013). Las TICs en la Educación. *Documento para la formación de Masters en TICs*. Jaén, Jaén, España.

Universidad Nacional de Colombia. (2003). *Guía para la elaboración de políticas de seguridad.* Colombia.

Universidad Perú. (s.f.). *http://www.universidadperu.com/telecomunicaciones-peru.php*. Recuperado el 24 de 11 de 2013, de universidaddel peru.com: http://www.universidadperu.com/telecomunicaciones-peru.php

Valero, A. (2008). *Taller del Congreso "Internet en el aula"*. Recuperado el 5 de 10 de 2013, de http://fresno.pntic.mec/avaler3

Vuelapluma, S. (2003). *Diccionario de Internet y Redes.* Madrid: McGraw-Hill/Interamericana.

Wordp. (2008). *Definición*. Recuperado el 6 de oct de 2013, de Definición de: http://definicion.de

Zayas, F., Esteve, P.P. (06 de 2010). docentes.leer.es. *Ciclo de Educación Primaria, T. Caza del tesoro*. Recuperado el 10 de 11 de 2013, de http://docentes.leer.es/files/2010/06/ep3_eso1_eso2_cazakiriko_prof_fzayas_pperez esteve.pdf

Bibliografía

Reglamento a la Ley Orgánica de Educación Intercultural. (31 de 03 de 2011). 109. Quito, Ecuador: Suplento registro oficial 417.

Aguilera, P. (s.f.). *Seguridad Informática.* (G. Morlanes, Ed.) Madrid, España: Editex.

Alegsa. (2012). *Diccionario de informática*. Recuperado el 22 de 06 de 2013, de http://www.alegsa.com.ar/Dic/seguridad%20informatica.php

Barroso, O. (2004). *La red como instrumento de búsqueda de información y comunicación.* Granada.

Bautista, L. (2013). *Plan de Seguridad de la Información.* España: Universitat Oberta de Catalunya. Recuperado el 9 de nov de 2013, de http://hdl.handle.net/10609/19443

Campusano Rodríguez, R. (2011). *Estudio, propuesta y aplicación de políticas de seguridad en los laboratorios de informática en las instituciones educativas de nivel básico.* Cuenca, Azuay, Ecuador: Universidad Tecnológica Israel.

Castells, M. (2010). *Sociedad Red* (Segunda ed.). Barcelona, España: UOC.

Chamorro, V. (2013). *Plan de Seguridad de la Información basado en el estandar ISO 13335 aplicado a un caso de estudio.* Quito, Pichincha, Ecuador: Escuela Politécnica Nacional.

Clayton, J. (2002). *Diccionario Ilustrado de telecomunicaciones.* McGraw-Hill.

Definición ABC. (2007). *Definición ABC*. Recuperado el 6 de 10 de 2013, de http://www.definicionabc.com/general/herramienta.php

Departamento de obras de referencia Ediciones Trébol,S.L. (2007). *Diccionario Enciclopédico.* Lima, Barcelona, España: Trébol, S.L.

Diario Hoy. (29 de abr de 2012). Menores expuestos a 7 amenazas en Internet. *Diario Hoy*.

Ecured. (27 de 10 de 2011). *http://www.ecured.cu/index.php/Telecomunicaciones*. Recuperado el 25 de 09 de 2013, de ecured.cu: http://www.ecured.cu/index.php/Telecomunicaciones

España, M. d. (12 de Feb de 2011). *Observatorio Tecnológico*. Recuperado el 2 de jun de 2013, de http://recursostic.educacion.es/observatorio/web/ca/cajon-de-sastre/38-cajon-de-sastre/961-monografico-redes-wifi?start=7

Gabavenda. (10 de nov de 2010). *La Teoría del bit*. Recuperado el 30 de jun de 2013, de http://lateoriadelbit.wordpress.com/2010/11/10/politica-de-seguridad-%E2%80%9Cmito-vs-realidad%E2%80%9D/

García, A., Huratado, C., & Alegre Ramos, P. (2011). *Seguridad Informática* (Primera ed.). Madrid, España: Paraninfo.

García, A., Hurtado, C., & Allegre, M. (2011). *Seguridad Informática* (Primera ed.). Madrid, España: Paraninfo.

Gobierno de Argentina. (11 de 2009). *ICIC Internet Sano.* Recuperado el 23 de 06 de 2013, de Programa nacional de infraestructuras críticas de información y ciberseguridad: http://www.internetsano.gob.ar/archivos/recomendaciones_navegacion_segura.pdf

Gobierno de la República del Ecuador. (2012). *Ley Orgánica de Educación Intercultural.* Quito, Ecuador.

Gobierno del Ecuador. (17 de 04 de 2002). Ley de Comercio Electrónico Firmas y Mensajes de Datos. (R. O. 557, Ed.) Quito, Pichincha, Ecuador. Recuperado el 6 de sep de 2013, de http://www.wipo.int/wipolex/en/text.jsp?file_id=243546

Gómez, Á. (2007). *Enciclopedia de la seguridad informática.* Alfaomega Grupo Editor.

Gómez, V. (2010). *Seguridad informática: básico.* Madrid: Starbook.

Goncalves, M. (2001). *Manual de firewalls.* McGraw-Hill.

Guazmayan, C. (2004). *El Internet y la investigación científica: el uso de los medios y las nuevas tecnologías en la educación.* Coop. Editorial Magisterio.

Gutierrez, J., & Tena, J. (s.f.). *Protocolos Criptográficos y Seguridad en Redes.* Universidad de Cantabria.

IEC/ITC 27005. (2008). *Normas ISO 27005.* Inglaterra.

IEC/ITC ISO 27001. (2005). *ISO 27001.* Inglaterra.

IETF. (sep de 1997). *The Internet Engineering Task Force (IETF).* Recuperado el 14 de jun de 2013, de http://www.ietf.org/rfc/rfc2196.txt: http://www.ietf.org/

ISO/ICE, ITC. (2005). *Normas ISO 27001.*

ISO/IEC. (13335-1:2004). ISO 13335-1.

ISO/IEC. (17799:2005).

ISO/IEC. (TR 18044:2004). *ISO 18044.*

Jaramillo, P. (20 de 08 de 2009). *SERENDIPITIC.* Recuperado el 7 de 10 de 2013, de http://ticserendipity.wordpress.com/2009/08/20/el-concepto-de-educacion/

Junta de Castilla y León - Consejería de Educación. (10 de 11 de 2013). *www.educa.jcyl.es*. Obtenido de http://www.educa.jcyl.es/ciberacoso/es/guias-informativas/guia-profesorado-centros-escolares

Larousse. (2009). Diccionario enciclopédico de la Lengua española. Larousse.

Lozano, J. (11 de 2008). *Investigación Exploratoria*. Recuperado el 30 de 06 de 2013, de http://janeth-investigacioniv.blogspot.com/2008/11/investigacion-exploratoria.html

Marañon, G. A. (2004). *Seguridad informática para empresas y particulares: el libro más completo y comprensible de seguridad informática para la empresa con aplicaicones, procedimientos y ejemplos prácticos para tomar decisiones relativas a la seguridad.* McGraw Hill Interamericana.

Matilla, A. (04 de 2013). *Blog de Seguridad Informática - Clase 1*. Recuperado el 22 de 06 de 2013, de http://www.agustinmantilla.com/clase-1-definicion-de-seguridad-informatica.html

Ministerio de Educación de Ecuador. (2013). *Educación básica*. Recuperado el 29 de jun de 2013, de http://educacion.gob.ec/educacion-general-basica/

Ministerio de Educación del Ecuador. (2013). *Educación Inicial*. Recuperado el 29 de jun de 2013, de Educación Inicial: http://educacion.gob.ec/educacion-inicial/

Ministerio de Inclusión Económica y Social. (09 de 2012). *Agenda para la igualdad de niños, niñas y adolescentes*. Recuperado el 22 de nov de 2013, de http://www.inclusion.gob.ec/wp-content/uploads/downloads/2012/09/master-agenda-ni%C3%B1ez-2da-edicion.pdf

Omerella, M. (s.f.). Recuperado el 29 de 09 de 2013, de http://www.iso27000.es/download/seguridad%20informaticavsinformacion.pdf

Ormella Meyer, C., & Asociados. (s.f.). ¿Seguridad informática vs. Seguridad de la información?

Patrick , D. (2003). *The Security Policy Life Cycle: Functions and Responsibilities.* Edited by Tipton & Krause, .

Pellejo, I., Andreu, F., & Lesta, A. (2006). *Fundamentos y aplicaciones de Seguridad en redes WLAN.* Barcelona: MARCOBO.

Poveda, J.M. (mar de 2011). *Los activos de seguridad de la información.* Recuperado el 27 de 10 de 2013, de Wordpress.com: http://jmpovedar.files.wordpress.com/2011/03/mc3b3dulo-7.pdf

Prudencio Aguado, D. (2012). *Seguridad Informática para el Hogar.* España: Bubok Pblishing S. L.

Pujadas I Jubany, J. (2008). *Seguridad Informática en Centros Educativos de Valladolid.* Valladolid. Recuperado el 8 de Junio de 2013, de http://www.bellera.cat/josep/pfsense/Valladolid-2008-07-03_v12.pdf

Quantum Ignis. (01 de 11 de 2013). *Quantum Ignis*. Recuperado el 23 de nov de 2013, de http://quantumignis.jimdo.com/articulos-t%C3%A9cnicos/incendios-de-origen-electrico/

Reese, B. (25 de 2 de 2011). *www.badreese.com.* Obtenido de http://www.bradreese.com/blog/2-25-2011.htm

Rodao, J. d. (2002). *Piratas cibernéticos: ciberwars, seguridad informática e internet* (2002 ed.). Alfaomega.

Rodriguez, D. M. (2002). *Sistemas Inalambricos de Comunicacion Personal.* Mexico: ALFAOMEGA.

RomeroTerreno, M. d., Barbancho Concejero, J., Berjumea Modejar, J., Rivera Romero, O., & Ropero Rodriguez, J. (2010). *Redes Locales* . Madrid: Parainfo,SA.

Rosique, R. (s.f.). *www.academia.edu.* Recuperado el 1 de 11 de 2013, de http://s3.amazonaws.com/academia.edu.documents/31001786/Un_asomo_a_la_Educacion_y_Web_1.pdf?AWSAccessKeyId=AKIAJ56TQJRTWSMTNPEA&Expires=1389028455&Signature=99FaoGCw2a%2Ba1OrAAv1nJQCnHhw%3D&response-content-disposition=inline

Segura, J. (2005). Internet en el aula las WebQuest. *Revista electrónica tecnológica educativa*(17).

Tewari, A. (6 de 2 de 2013). *www.sisainfosec.com.* Recuperado el 7 de 10 de 2013, de http://sisainfosec.com/blog/comparison-between-iso-27005-octave-nist-sp-800-30-2/

UNESCO. (2010). unesco. *Conclusiones de TICs en la Educación.* Recuperado el 1 de junio de 2013, de Unesco: http://unesdoc.unesco.org/images/0019/001905/190555s.pdf

Universidad de Jaén. (2013). Las TICs en la Educación. *Documento para la formación de Masters en TICs*. Jaén, Jaén, España.

Universidad Nacional de Colombia. (2003). *Guía para la elaboración de políticas de seguridad.* Colombia.

Universidad Perú. (s.f.). *http://www.universidadperu.com/telecomunicaciones-peru.php*. Recuperado el 24 de 11 de 2013, de universidaddel peru.com: http://www.universidadperu.com/telecomunicaciones-peru.php

Valero, A. (2008). *Taller del Congreso "Internet en el aula"*. Recuperado el 5 de 10 de 2013, de http://fresno.pntic.mec/avaler3

Vuelapluma, S. (2003). *Diccionario de Internet y Redes.* Madrid: McGraw-Hill/Interamericana.

Wordp. (2008). *Definición*. Recuperado el 6 de oct de 2013, de Definición de: http://definicion.de

Zayas, F., Esteve, P.P. (06 de 2010). docentes.leer.es. *Ciclo de Educación Primaria, T. Caza del tesoro*. Recuperado el 10 de 11 de 2013, de http://docentes.leer.es/files/2010/06/ep3_eso1_eso2_cazakiriko_prof_fzayas_pperez esteve.pdf

Glosario de términos

"Aceptación de riesgo es la decisión de aceptar el riesgo (ISO/IEC Guía 73:2002)" (ISO/ICE, ITC, 2005, pág. 11) .

"Análisis de riesgo uso sistemático de la información para identificar fuentes y para estimar el riesgo (ISO/IEC Guía 73:2002)" (ISO/ICE, ITC, 2005, pág. 11).

"Evaluación del riesgo es proceso de comparar el riesgo estimado con el criterio de riesgo dado para determinar la importancia del riesgo. (ISO/IEC Guía 73:2002)" (ISO/ICE, ITC, 2005, pág. 11).

"Enunciado de aplicabilidad es un documento que describe los objetivos de control y los controles que son relevantes y aplicables al SGSI de la organización" (ISO/ICE, ITC, 2005, pág. 12).

"Gestión de riesgo son actividades coordinadas para dirigir y controlar una organización con relación al riesgo (ISO/IEC Guía 73:2002)" (ISO/ICE, ITC, 2005, pág. 11).

"Riesgo residual es el riesgo remanente después del tratamiento del riesgo (ISO/IEC Guía 73:2002)" (ISO/ICE, ITC, 2005, pág. 11).

"Tratamiento del riesgo es el proceso de tratamiento de la selección e implementación de medidas para modificar el riesgo (ISO/IEC Guía 73:2002)" (ISO/ICE, ITC, 2005, pág. 11).

"Valuación del riesgo es el proceso general de análisis del riesgo y evaluación del riesgo" (ISO/IEC Guía 73:2002)". (ISO/ICE, ITC, 2005, pág. 11).

ANEXOS

Anexo 1: Guía de Visitas Técnicas realizadas en el CELP

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

MAESTRÍA EN REDES Y TELECOMUNICACIONES

GUÍA DE VISITA TÉCNICA REALIZADA EN EL CENTRO EDUCATIVO LA PRADERA

Objetivo: Obtener información de la dimensión software del CELP.

Fecha:	**Nombre de quien realiza la visita técnica**
Hora de inicio:	**Hora de finalización:**
Responsables de la visita:	
Actividades realizadas:	
Observaciones:	

Anexo 2: Encuesta dirigida al Personal Docente referente a valoración de activos

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

MAESTRÍA EN REDES Y TELECOMUNICACIONES

ENCUESTA DIRIGIDA AL PERSONAL DOCENTE Y ADMINISTRATIVO DEL CENTRO EDUCATIVO LA PRADERA

Objetivo: Realizar una Valoración de Activos tomando en cuenta los parámetros de disponibilidad, confidencialidad, integridad para realizar el análisis de amenazas y riesgos para la institución.

Instructivo: Conteste a las preguntas con sinceridad en base a la siguiente tabla de valores

1. **DISPONIBILIDAD**

VALOR	CRITERIO
0	No aplica o no es relevante
1	Debe estar disponible al menos el 10% de tiempo
2	Debe estar disponible al menos el 50% de tiempo
3	Debe estar disponible al menos el 99% de tiempo

¿Cuál sería la importancia o el trastorno que tendría que el Activo que tiene a cargo o que maneja no estuviera disponible? _____

¿Cuál sería la importancia o el trastorno que tendría que el Servicio de Internet no esté disponible? _____

¿Cuál sería la importancia o el trastorno que tendría que el Servidor de Aplicaciones donde se encuentra alojado el Sistema para la Gestión de la Información del Centro Educativo La Pradera no esté disponible? _____

¿Cuál sería la importancia o el trastorno que tendría que el Servicio Telefónico del Centro Educativo La Pradera no esté disponible? _____

¿Cuál sería la importancia o el trastorno que tendría que la Página Web del Centro Educativo La Pradera no esté disponible? _____

¿Cuál sería la importancia o el trastorno que tendría que la Información del Centro Educativo La Pradera no esté disponible cuando se necesite hacer uso de la misma? _____

¿Cuál sería la importancia o el trastorno que tendría que las computadoras utilizadas en el Laboratorio de TICs del Centro Educativo La Pradera no estén disponibles para el aprendizaje de los estudiantes? _____

¿Cuál sería la importancia o el trastorno que tendría que los activos no estén disponibles por negligencia (olvido de la ubicación, no disponer de un inventario codificado adecuadamente, no disponer de recursos adecuados para el almacenamiento, entre otros) en el manejo de los mismos en el Centro Educativo La Pradera? _____

¿Cuál sería la importancia o el trastorno que tendría que el servicio de Energía eléctrica no esté disponible el Centro Educativo La Pradera? _____

¿Cuál sería la importancia o el trastorno que tendría que el servicio Wifi no esté disponible en el Centro Educativo La Pradera? _____

2. **INTEGRIDAD**

VALOR	CRITERIO
0	No aplica o no es relevante
1	No es relevante los errores que tenga la información que falte
2	Tiene que estar correcto o completo al menos 50%
3	Tiene que estar correcto o completo al menos 95%

¿Qué importancia tendría que el activo que usted maneja o del que está a cargo fuera alterado sin autorización ni control? _____

¿Qué importancia tendría que en el servidor de aplicaciones (Sistema de Gestión de Información del Centro Educativo La Pradera) fueran modificado, por personal no autorizado, las cuentas de usuario.

3. **CONFIDENCIALIDAD**

VALOR	CRITERIO
0	No aplica o no es relevante
1	Daños muy bajos, el incidente no trascendería al área afectada
2	Serían relevantes, el incidente no aplicaría a otras áreas
3	Los daños serían catastróficos, la reputación y la imagen se verían comprometidos

¿Cuál sería la importancia que el activo que usted maneja o tiene a su cargo fuera accedido de manera no autorizada?

¿Cuál sería la importancia que las claves de acceso al sistema que le sean entregadas estén en manos de otras personas que no sea usted?

¿Cuál sería la importancia que los programas instalados en los computadores del laboratorio de Tics fuesen modificados o borrados de los equipos?

Anexo 3: Encuesta dirigida a los estudiantes referente a Valoración de Activos

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

MAESTRÍA EN REDES Y TELECOMUNICACIONES

ENCUESTA DIRIGIDA A LOS ESTUDIANTES DEL CENTRO EDUCATIVO LA PRADERA

Objetivo: Realizar una Valoración de Activos tomando en cuenta los parámetros de disponibilidad, confidencialidad, integridad para realizar el análisis de amenazas y riesgos para la institución.

Instructivo: Conteste a las preguntas con sinceridad en base a la siguiente tabla de valores

1. **DISPONIBILIDAD**

VALOR	CRITERIO
0	No aplica o no es relevante
1	Debe estar disponible al menos el 10% de tiempo
2	Debe estar disponible al menos el 50% de tiempo
3	Debe estar disponible al menos el 99% de tiempo

¿En qué porcentaje usted considera que debe estar disponible el Internet en el Laboratorio cuando lo necesita? _____

¿Cuál sería la importancia que tendría que la Página Web del Centro Educativo La Pradera no esté disponible? _____

¿Cuál sería la importancia o el trastorno que tendría que las computadoras utilizadas en el Laboratorio de Tics del Centro Educativo La Pradera no estén disponibles para el aprendizaje de los estudiantes? _____

2. **INTEGRIDAD**

VALOR	CRITERIO
0	No aplica o no es relevante
1	No es relevante los errores que tenga la información que falte
2	Tiene que estar correcto o completo al menos 50%
3	Tiene que estar correcto o completo al menos 95%

¿Qué importancia tendría que el computador que usted maneja en el laboratorio fuera alterado sin autorización ni control? _____

3. **CONFIDENCIALIDAD**

VALOR	CRITERIO
0	No aplica o no es relevante
1	Daños muy bajos, el incidente no trascendería al área afectada
2	Serían relevantes, el incidente no aplicaría a otras áreas
3	Los daños serían catastróficos, la reputación y la imagen se verían comprometidos

¿Qué pasaría si los programas instalados en los computadores del laboratorio de Tics que usted utiliza fuesen modificados o borrados de los equipos?

Anexo 4: Encuesta dirigida a los docentes referente a Educación

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

MAESTRÍA EN REDES Y TELECOMUNICACIONES

ENCUESTA DIRIGIDA A LOS DOCENTES DEL CENTRO EDUCATIVO LA PRADERA

Objetivo: Conocer el uso del Internet como Herramienta de Apoyo en la formación de niños, niñas y adolescentes del Centro Educativo La Pradera.

Instructivo: Conteste a las preguntas con sinceridad en base a la siguiente tabla de valores

EDUCACIÓN

INTERNET

¿Tiene acceso a Internet en la Institución?

Si_____ No _____ A veces _____

¿Cuándo usted usa el Internet tiene la precaución de dirigir la consulta o investigación a sitios seguros?

Si_____ No _____ Tal vez _____ No se _____

Considera usted que el Internet ayudaría a la formación académica

Si_____ No _____ Tal vez _____ No se _____

¿Existe en la Institución alguna política, norma, estándar o procedimiento para solicitar el uso de Internet?

Si_____ No _____ Tal vez _____ No se _____

TIC

¿Usted utiliza Software educativo para dictar sus clases?

Si_____ No_____ Tal vez _____ Nunca _____

¿Cree usted que los recursos tecnológicos con que cuenta la Institución son adecuados para utilizarlos como herramienta en la formación de los alumnos?

Si_____ No _____ Tal vez _____

¿Considera que las TIC son de ayuda para la educación de los alumnos de la Institución?

Si_____ No _____ Tal vez _____

¿Le gustaría que le capaciten en el uso de herramientas orientadas a las TICs en el Internet?

Si _____ No _____ Tal vez _____

COMPUTADORES

¿Dispone de un computador para realizar sus investigaciones en Internet en la Institución?

Si_____ No _____ A veces _____

¿Existe alguna política, norma, estándar o procedimiento para solicitar el uso de Laboratorio para dar sus clases?

Si_____ No _____ Tal vez _____ No se _____

¿Tiene conocimiento si existe alguna política, norma, estándar o procedimiento para garantizar seguridad informática en el Centro Educativo La Pradera?

Si_____ No _____ Tal vez _____ No se _____

Anexo 5: Encuesta dirigida a los padres de familia referente a Educación

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

MAESTRÍA EN REDES Y TELECOMUNICACIONES

ENCUESTA DIRIGIDA A LOS PADRES DE FAMILIA DEL CENTRO EDUCATIVO LA PRADERA

Objetivo: Conocer el uso del Internet como Herramienta de Apoyo en la formación de niños, niñas y adolescentes del Centro Educativo La Pradera.

Instructivo: Conteste a las preguntas con sinceridad en base a la siguiente tabla de valores

EDUCACIÓN

¿Sabe usted si el profesor de su niño utiliza Internet para dictar sus clases?

Si_____ No_____ Tal vez _____ No se _____

¿Sabe usted si existen parámetros de seguridad de acceso al Internet en el Centro Educativo La Pradera?

Si_____ No_____ Tal vez _____ No se _____

¿Sabe usted de alguna herramienta en la cual bloquee los accesos indebidos en Internet?

Si_____ No_____ Tal vez _____ No se _____

¿Considera usted que los computadores que su hijo usa en el Laboratorio son adecuados para utilizar durante las clases?

Si_____ No_____ Tal vez _____ No se _____

¿Su hijo tiene acceso a Internet en el Laboratorio?

Si_____ No_____ Tal vez _____ No se _____

¿Existe alguna forma para solicitar el uso de Laboratorio en horas libres?

Si_____ No _____ Tal vez _____ No se _____

Anexo 6: Guía de la Entrevista dirigida al Encargado de Tecnología

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

MAESTRÍA EN REDES Y TELECOMUNICACIONES

ENTREVISTA DIRIGIDA AL ENCARGADO DE TECNOLOGÍA Y PROPIETARIO DEL CENTRO EDUCATIVO LA PRADERA

Objetivo: Indagar sobre el manejo de respaldos de la información

PREGUNTA	**RESPUESTA** **Encargado de Tecnología**	**RESPUESTA** **Propietario**
¿Quién es el encargado de respaldar la información?		
¿Realizan copias de seguridad de la información en forma periódica?		
¿Existen definidos procedimientos para realizar copias de seguridad de la información?		
¿Existe un lugar seguro fuera de la institución donde permanezca una copia de los respaldos de la información?		
¿Cuenta la institución con un plan de contingencia ante recuperación de desastres?		

Tabla A.1: Guía de la Entrevista dirigida al encargado de tecnología y propietario sobre manejo de respaldos (Elaborado por: Investigador)

ENTREVISTA DIRIGIDA AL ENCARGADO DE TECNOLOGÍA Y PROPIETARIO DEL CENTRO EDUCATIVO LA PRADERA

Objetivo: Indagar sobre el control de acceso a Internet

PREGUNTA	RESPUESTA Encargado de Tecnología	RESPUESTA Propietario
¿Los docentes tienen acceso a Internet?		
¿Existen políticas que permitan hacer un uso adecuado del Internet?		
¿Existen bitácoras del control de uso de Internet en el Laboratorio de computación?		
¿Existe algún procedimiento para que un docente que no sea el profesor de computación, utilice el laboratorio?		
¿Existe algún procedimiento para autorización de ingreso o salida de equipos fuera del laboratorio de TICs o de la Institución?		
¿Tiene algún mecanismo que permita compartir Internet de manera segura y además que evite el acceso a sitios web que se encuentran en listas negras?		

Tabla A.2: Guía de entrevista dirigida al encargado de tecnología y al propietario sobre control de acceso a Internet
(Elaborado por: Investigador)

Anexo 7: Guía de la Entrevista dirigida al Encargado de Tecnología y al desarrollador del Sistema de Gestión de Información

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

MAESTRÍA EN REDES Y TELECOMUNICACIONES

ENTREVISTA DIRIGIDA AL Encargado de Tecnología, Desarrollador del Sistema y Propietario DEL CENTRO EDUCATIVO LA PRADERA

Objetivo: Indagar sobre las seguridades que tiene el Sistema de Gestión de Información y la Base de datos

Pregunta	**Respuesta Encargado de Tecnología**	**Respuesta Desarrollador**	**Respuesta Propietario**
¿Existen políticas para la asignación de usuarios y perfiles de acceso?			
¿Son las contraseñas almacenadas usando algún método de encriptación?			
¿Existe políticas que aseguren el acceso a la información a la Base de Datos?			

Tabla A.3: Guía de la Entrevista dirigida al Encargado de Tecnología, Desarrollador y Propietario sobre Sistema de gestión de información y base de datos (Elaborado por: Investigador)

Anexo 8: Entrevista dirigida a la Jefatura de Talento Humano

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

MAESTRÍA EN REDES Y TELECOMUNICACIONES

ENREVISTA DIRIGIDA A LA JEFATURA DE TALENTO HUMANO DEL CENTRO EDUCATIVO LA PRADERA

Objetivo: Indagar sobre las responsabilidades, roles del personal docente y administrativo en lo que respecta a la seguridad informática

Pregunta	Respuesta
¿Tiene definido roles y responsabilidades de seguridad informática de los empleados, estudiantes, padres de familia, terceros?	
¿Tienen establecido en el contrato de trabajo el personal los roles y responsabilidades y las de la organización para la seguridad de información?	

Tabla A.4: Guía de entrevista a Jefe de Talento Humano sobre roles y responsabilidades de seguridad informática (Fuente: Propia)

Objetivo: Indagar si el elemento humano está al tanto sobre amenazas, inquietudes sobre la seguridad de la información

PREGUNTA	RESPUESTA
¿Tienen definidas políticas y procedimientos en donde se garantice la aplicación de Gestión de Responsabilidades	
¿Reciben los empleados capacitaciones en lo que respecta a seguridad de la información?	
¿Existe algún proceso disciplinario cuando algún empleado ha cometido alguna violación en la seguridad?	
¿Están claramente definidas las responsabilidades a la terminación o cambio de empleo en cuanto a seguridad de información?	
¿Los empleados devuelven todos los activos al terminar sus funciones?	
¿Cuál es el proceso de eliminación de derechos de acceso cuando un empleado termina sus funciones?	

Tabla A.5: Guía de la Entrevista a la Jefatura de Talento Humano sobre amenazas y el talento humano, sobre seguridad informática (Fuente: Propia)

Anexo 9: Fotografías de amenazas

Pared húmeda en el Laboratorio

Gráfico: A.1 Fotografía de Pared húmeda del Laboratorio Tics(Elaborado por: Investigador)

Ubicación de los equipos en el espacio físico del Laboratorio de Tics

Gráfico: A.2 Laboratorio Tics Bloque 1(Elaborado por: Investigador)

Susceptibilidad al polvo

Gráfico: A.3 Fotografía de CPU sin tapas frontales (Elaborado por: Investigador)

Susceptibilidad a la suciedad

Gráfico: A.4 Fotografía donde se evidencia basura y CPU sin tapas posteriores (Elaborado por:Investigador)

Instalaciones eléctricas

Gráfico: A.5 Fotografía en la se puede observar cables en el piso (Elaborado por: Investigador)

No existe vidrio en la puerta del laboratorio

Gráfico: A.6 Fotografía de puerta del Laboratorio sin vidrio (Elaborado por: Investigador)

Cable telefónico cortado en la terraza de la Institución

Gráfico: A.7 Fotografía de cable telefónico roto en la terraza del Bloque 2 (Elaborado por: Investigador)

Tarjeta de red mal colocada

Gráfico: A.8 Fotografía en la que se evidencia una tarjeta de red inalámbrica mal colocada (Elaborado por: Investigador)

Drivers no instalados de la interface de red

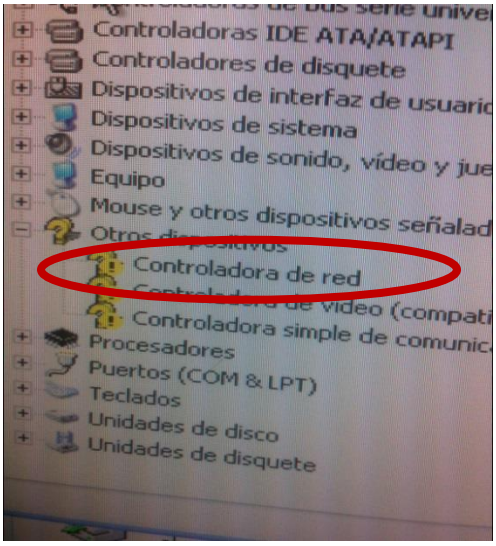


Gráfico: A.9 Fotografía en la que se evidencia que la tarjeta de red no está bien instalada (Elaborado por: Investigador)

Equipos de comunicación abandonados por 8 meses sin conectar

Gráfico: A.10 Dispositivos de comunicaciones arrumados por 8 meses sin utilizar (Elaborado por: Investigador)

Anexo 10 Fotografías de socialización con el personal de la Institución

Gráfico: A.11 Fotografía en la que se trabaja Proyecto de Capacitación TICs Docentes (Elaborado por: Investigador)

Anexo 11: Incidencias de cortes del servicio de Internet

Servicio de Internet

Fecha	Número de incidencia asignada CNT	Descripción Incidencia	Observación
1-feb-2013 a 8-oct-2013	No anotan el número de incidencia	Reporta: Lic. Edwin Alarcón Problema: No hay Internet , modem dañado Observación: Problema de la conexión en la Institución Estado: Cerrado	Nadie hace el seguimiento y la CNT dice que no es problema del modem
12-oct-13	19452854	Reporta: Ing. Tannia Mayorga Problema: No hay Internet Descripción: Línea cortada en el poste Estado: Cerrado	No hay solución, reportan que la línea telefónica está bien
15-oct-13	19490907	Botón foco ADSL apagado Reporta: Ing. Tannia Mayorga Problema: No hay Internet Descripción: Línea cortada en el poste Estado: Cerrado	No hay solución, reportan que la línea telefónica está bien y que llaman y no contesta nadie

Tabla A6: Incidencias del servicio de Internet (cont.)

Tabla A6: Incidencias del servicio de Internet (cont.)

Fecha	Número de incidencia asignada CNT	Descripción Incidencia	Observación
18-oct-13	291479	Botón foco ADSL apagado Reporta: Ing. Tannia Mayorga Problema: No hay Internet Observación: Visita realizada Estado: Cerrado	No hay solución, reportan que la línea telefónica está bien
18-oct-13	19497521	Botón foco ADSL apagado Reporta: Ing. Tannia Mayorga Problema: No hay Internet Descripción: Línea cortada en el poste Estado: Cerrado	19 de octubre soluciona la CNT arreglando la línea telefónica
27-oct-13	19545968	Botón foco Internet apagado Reporta: Ing. Tannia Mayorga Problema: No hay Internet Estado: Cerrado	No hay solución, reportan visita por daño de modem

Tabla A6: Incidencias del servicio de Internet (cont.)

Tabla A6: Incidencias del servicio de Internet (cont.)

Fecha	Número de incidencia asignada CNT	Descripción Incidencia	Observación
30-oct-13	19570800	Botón foco ADSL apagado Reporta: Ing. Tannia Mayorga Problema: No hay Internet Descripción: Línea cortada en el poste Estado: Cerrado	Reportan caso cerrado porque no hay quien abra para revisión, se solicita otra visita, revisan el modem sin arreglo alguno
04-nov-13	No reportan	No hay Internet, llega por 1 hora y se corta el resto del día	Nadie hace el seguimiento en la CNT
05-nov-13	No entregan número	Hay Internet 1 hora y se corta	Coloca la CNT filtros de ruido en la extensión y en el laboratorio. No hay seguimiento
06-nov-13	No reportan	No hay Internet	Nadie hace el seguimiento en la CNT
07-nov-13	No reportan	No hay Internet	Nadie hace el seguimiento en la CNT

Tabla A6: Incidencias del servicio de Internet (cont.)

Tabla A6: Incidencias del servicio de Internet (cont.)

Fecha	Número de incidencia asignada CNT	Descripción Incidencia	Observación
08-nov-13	No hay número de incidencia	Botón foco Internet apagado	El técnico revisa el modem, con Ing. Tannia Mayorga, configura otra vez el usuario, resetea la contraseña, y manifiesta que el usuario original es con andinanet y que estaba con fastboy, luego de ello hay internet
11-nov-13	No reportan	Reporta: Ing. Tannia Mayorga	Nadie hace el seguimiento en la CNT
13-nov-13	No reportan	Problema: No hay Internet	Nadie hace el seguimiento en la CNT
15-nov-13	No reportan	Descripción: El foco de ADSL ya funciona pero no hay Internet, hay unos cinco minutos y luego se corta por horas, regresa unos diez minutos y se vuelve a cortar Estado: Cerrado	Nadie hace el seguimiento en la CNT

Tabla A.6: Incidencias de cortes del servicio de Internet (Elaborado por: Investigador)

Anexo 12: Incidencias de problemas de conexión a la red en el área administrativa

Fecha	Número	Usuario	Incidencia	Observación
7/10/2013	001	Secretaria	No funciona el sistema	Al revisar es problema de red ya que está apagado el switch
8/10/2013	002	Secretaria	Se queda el sistema colgado	No se puede prender el switch ya que está cerrada la oficina de los Propietarios
9/10/2013	003	DOBE	No ingresa a Internet	Está apagado el switch por lo que no pueden navegar y la oficina de los propietarios está cerrada
10/10/2013	004	Inspección	No ingresa al Internet	Está cerrada la oficina de los propietarios y no se puede encender el switch
11/10/2013	005	Secretaria	No tengo Internet	Quemada la tarjeta de red ya que cayó un rayo y se quemó, se comunica al propietario para la reposición
14/10/2013	006	Secretaria	No puedo ingresar al sistema	No está prendido el servidor de aplicaciones ni tampoco el switch de la red ya que no tiene acceso a la oficina de los propietarios
15/10/2013	007	Docente	Quiero ingresar a la página del	Está apagado el switch y la oficina de los propietarios

Tabla A.7: Incidencias de problemas de conexión en la red del área administrativa (cont.)

Tabla A.7: Incidencias de problemas de conexión en la red del área administrativa (cont.)

			ministerio de educación y no vale	pasa cerrada.
16/10/2013	008	Secretaria	Se demora en ingresar al sistema más de 15 minutos	Problemas de configuración de red y servicios web.
17/102013	009	Secretaria	No puedo hacer nada en el sistema porque no ingresa	Problemas de configuración de red y servicios web
10/10/2013	010	Inspección	No puedo imprimir	Problemas de configuración de red
21/10/2013	011	Docentes	No puede navegar	Switch apagado, no hay acceso a la oficina de los propietarios
22/10/2013	012	Secretaria	No puede navegar	Switch apagado, no hay acceso a la oficina de los propietarios
23/10/2013	013	Secretaria	Se sigue demorando el ingreso al sistema	El desarrollador manifiesta que ya se va a conectar para ver que pasa
24/10/2013	014	Secretaria	No puedo ingresar al sistema	Equipos de comunicación apagados
25/10/2013	015	Secretaria	No puedo ingresar al sistema	Equipos de comunicación apagados
26/10/2013 27/10/2013	016 017	Secretaria	No puedo ingresar al sistema	Equipos de comunicación apagados

Tabla A.7: Incidencias de problemas de conexión a la red en el área administrativa
(Elaborado por: Investigador)

Anexo 13: Niños, niñas y adolescentes que sufren algún tipo de delito a través de plataformas virtuales

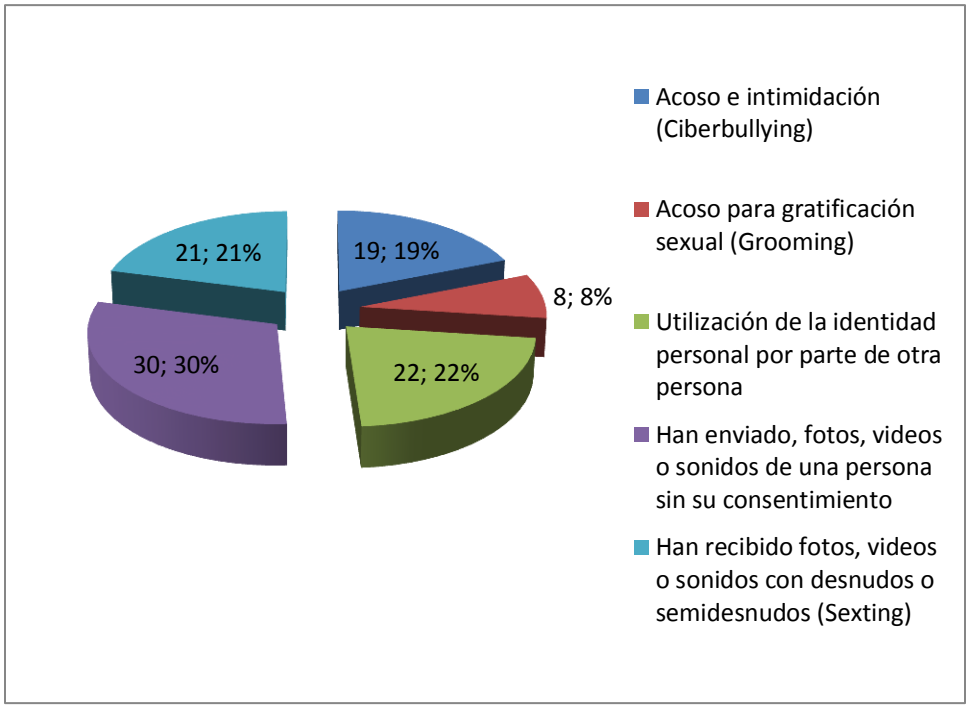


Gráfico: A.12 Niños. niñas y adolescentes que sufren algún tipo de delito a través de plataformas virtuales (Ministerio de Inclusión Económica y Social, 2012)

Fuente y elaboración: CNNA-MIES,2011

En la investigación realizada por la CNNA conjuntamente con el MIES (2011), en 12 instituciones educativas del país, detectó que 12 de cada 100 adolescentes sufre de acoso e intimidación a través de plataformas virtuales. Asimismo, indica que 5 de cada 10 adolescentes sufren de acoso para gratificación sexual (Ministerio de Inclusión Económica y Social, 2012)

Anexo 14: Sección de Log del 5 del nov 9:17 Estudiantes de 5to-6to-7mo donde se ven accesos no adecuados

```
1383659242.031    406 192.168.2.5 TCP_MISS/200 963 GET
http://www.code.org/ - DIRECT/66.254.102.216 text/html
1383659242.781    266 192.168.2.7 TCP_MISS/200 349 GET
http://186.42.193.235/pagead/ads.js? - DIRECT/186.42.193.235
application/x-javascript
1383659246.234   3344 192.168.2.5 TCP_MISS/200 535 GET
http://resources.crossrider.com/apps/43914/resources/meta/1? -
DIRECT/69.16.175.10 text/html
1383659248.921   6437 192.168.2.5 TCP_MISS/200 8577 GET
http://www.playboy.com/ - DIRECT/66.254.102.216 text/html
1383659252.031   1063 192.168.2.5 TCP_MISS/200 1689 GET
http://static2.playboy.com/assets/tour/js/base/oas-ads.js? -
DIRECT/8.254.10.253 application/javascript
1383659252.156   1203 192.168.2.5 TCP_MISS/200 4911
GET http://notify6.dropbox.com/subscribe? - DIRECT/108.160.163.42
text/plain
1383659349.078    219 192.168.2.2 TCP_MISS/204 383 GET
http://b.scorecardresearch.com/b? - DIRECT/186.46.140.211 -
1383659349.125    469 192.168.2.3 TCP_MISS/500 1061 GET
http://www.tudiscoverykids.com/dni-tvlistings/GetScheduleByTime? -
DIRECT/186.46.140.224 text/html
1383659349.203    328 192.168.2.3 TCP_MISS/302 908 GET
http://googleads.g.doubleclick.net/pagead/viewthroughconversion/991498
594/? - DIRECT/173.194.37.13 text/html
1383659349.265    390 192.168.2.3 TCP_MISS/200 1568 GET
http://ad.doubleclick.net/N5081/adj/dla.es.kids/home;sz=160x600,120x60
0;ord=7291373030696211? - DIRECT/173.194.37.27 text/javascript
1383659349.359    500 192.168.2.3 TCP_MISS/200 1929 POST
http://safebrowsing.clients.google.com/safebrowsing/downloads? -
DIRECT/173.194.37.2 application/vnd.google.safebrowsing-update
1383659349.390    531 192.168.2.8 TCP_MISS/302 1004 GET
http://www.google.com/ads/user-lists/991498594/? -
DIRECT/173.194.37.17 text/html
1383659351.015  10594 192.168.2.9 TCP_MISS/200 63367 CONNECT dl-
debug19.dropbox.com:443 - DIRECT/107.20.249.78 -
1383659351.781    235 192.168.2.2 TCP_MISS/200 562 GET
http://www.google-analytics.com/__utm.gif? - DIRECT/173.194.37.103
image/gif
1383659352.093    437 192.168.2.5 TCP_MISS/200 1016 GET
http://www.playboy.com/gallery/view/elizabeth-marxs-texas-climax -
DIRECT/66.254.102.216 text/html
1383659353.093      0 192.168.2.10 TCP_NEGATIVE_HIT/500 1067 GET
http://www.tudiscoverykids.com/dni-tvlistings/GetScheduleByTime? -
NONE/- text/html
```

```
1383659353.531    360 192.168.2.5 TCP_MISS/200 349 GET
http://186.42.193.235/pagead/ads.js? - DIRECT/186.42.193.235
application/x-javascript
1383659353.890    719 192.168.2.5 TCP_MISS/200 12176 GET
http://www.playboy.com/gallery/view/elizabeth-marxs-texas-climax -
DIRECT/66.254.102.216 text/html
1383659354.953    250 192.168.2.3 TCP_MISS/200 10953 GET
http://safebrowsing-
cache.google.com/safebrowsing/rd/ChNnb29nLW1hbHdhcmUtc2hhdmFyEAEY98kHI
IDKBzIG9-QBAP8D - DIRECT/173.194.37.1
application/vnd.google.safebrowsing-chunk
1383659355.765      0 192.168.2.7 TCP_NEGATIVE_HIT/500 1067 GET
http://www.tudiscoverykids.com/dni-tvlistings/GetScheduleByTime? -
NONE/- text/html
1383659356.000   1000 192.168.2.5 TCP_REFRESH_HIT/304 328 GET
http://static2.playboy.com/assets/tour/js/vendor/jquery.migrate.js? -
DIRECT/8.254.10.253 -
1383659356.031   1016 192.168.2.5 TCP_REFRESH_HIT/304 329 GET
http://static2.playboy.com/assets/tour/js/base/firstload.js? -
DIRECT/199.93.36.254 -
1383659356.062   1047 192.168.2.5 TCP_REFRESH_HIT/304 328 GET
http://static2.playboy.com/assets/tour/js/base/oas-ads.js? -
DIRECT/8.26.201.125 -
1383659356.218   3140 192.168.2.3 TCP_MISS/302 1002 GET
http://www.google.com/ads/user-lists/991498594/? -
DIRECT/173.194.37.17 text/html
1383659356.906    797 192.168.2.11 TCP_MISS/200 24023 GET
http://safebrowsing-
cache.google.com/safebrowsing/rd/ChNnb29nLW1hbHdhcmUtc2hhdmFyEAEYgcoHI
IDUByqhARzlAQD_____
_____
_____
__________8fMggB5QEA____Bw - DIRECT/173.194.37.1
application/vnd.google.safebrowsing-chunk
1383659356.921   1281 192.168.2.6 TCP_MISS/200 604 GET
http://www.google.com.ec/ads/user-lists/991498594/? -
DIRECT/173.194.37.31 text/html
1383659356.953   1313 192.168.2.3 TCP_MISS/302 727 GET
http://c.brightcove.com/services/viewer/federated_f9? -
DIRECT/64.74.101.75 -
1383659357.078  65250 192.168.2.6 TCP_MISS/200 4122 CONNECT
platform.twitter.com:443 - DIRECT/23.7.113.224 -
1383659358.187    375 192.168.2.3 TCP_MISS/200 31988 GET
http://safebrowsing-
cache.google.com/safebrowsing/rd/ChNnb29nLW1hbHdhcmUtc2hhdmFyEAAY-
fcHIKD4BzIK-fsBAP_____AA - DIRECT/173.194.37.1
application/vnd.google.safebrowsing-chunk
1383659358.593    281 192.168.2.7 TCP_MISS/200 6215 GET
http://safebrowsing-
```

```
cache.google.com/safebrowsing/rd/ChNnb29nLW1hbHdhcmUtc2hhdmFyEAAYofgHI
MD5ByoWNvwBAP_____BzIHIfwBAP__Hw - DIRECT/173.194.37.1
application/vnd.google.safebrowsing-chunk
1383659358.625   3625 192.168.2.5 TCP_REFRESH_HIT/304 329 GET
http://static2.playboy.com/assets/tour/js/vendor/jquery.min.js? -
DIRECT/8.26.201.125 -
1383659359.062    187 192.168.2.3 TCP_MISS/200 969 GET
http://safebrowsing-
cache.google.com/safebrowsing/rd/ChFnb29nLXBoaXNoLXNoYXZhchABGJedCSCgn
QkyBpdOAgD_Aw - DIRECT/173.194.37.1
application/vnd.google.safebrowsing-chunk
1383659359.093   4047 192.168.2.17 TCP_MISS/200 10278 GET
http://static2.playboy.com/assets/tour/css/galleries.css -
DIRECT/8.254.10.253 text/css
1383659359.109   3469 192.168.2.3 TCP_MISS/302 1004 GET
http://www.google.com/ads/user-lists/991498594/? -
DIRECT/173.194.37.18 text/html
1383659359.703   3375 192.168.2.3 TCP_MISS/302 727 GET
http://c.brightcove.com/services/viewer/federated_f9? -
DIRECT/64.74.101.75 -
1383659359.734    188 192.168.2.3 TCP_CLIENT_REFRESH_MISS/200 2030 GET
http://safebrowsing-
cache.google.com/safebrowsing/rd/ChFnb29nLXBoaXNoLXNoYXZhchABGKGdCSDAn
gkqFrhOAgD_____wEyB6FOAgD__38 - DIRECT/173.194.37.1
application/vnd.google.safebrowsing-chunk
1383659359.796   4156 192.168.2.7 TCP_MISS/302 727 GET
http://c.brightcove.com/services/viewer/federated_f9? -
DIRECT/64.74.101.75 -
1383659359.796    234 192.168.2.3 TCP_MISS/200 604 GET
http://www.google.com.ec/ads/user-lists/991498594/? -
DIRECT/173.194.37.31 text/html
1383659360.203    266 192.168.2.7 TCP_MISS/200 3101 GET
http://admin.brightcove.com/viewer/us20131121.1403/BrightcoveBootloade
r.swf? - DIRECT/186.46.140.217 application/x-shockwave-flash
1383659360.218   3203 192.168.2.3 TCP_MISS/200 3101 GET
http://admin.brightcove.com/viewer/us20131121.1403/BrightcoveBootloade
r.swf? - DIRECT/186.46.140.203 application/x-shockwave-flash
1383659360.390    219 192.168.2.3 TCP_MISS/200 16464 GET
http://safebrowsing-
cache.google.com/safebrowsing/rd/ChFnb29nLXBoaXNoLXNoYXZhchAAGJ3LEiCwy
xIyB52lBAD__w8 - DIRECT/173.194.37.1
application/vnd.google.safebrowsing-chunk
1383659363.171    578 192.168.2.6 TCP_MISS/200 48883 GET
http://safebrowsing-
cache.google.com/safebrowsing/rd/ChFnb29nLXBoaXNoLXNoYXZhchAAGLHLEiCAz
BIqCOelBAD___8DMguxpQQA________Pw - DIRECT/173.194.37.1
application/vnd.google.safebrowsing-chunk
```

```
1383659364.625   9641 192.168.2.9 TCP_REFRESH_HIT/304 330 GET
http://static2.playboy.com/assets/tour/css/common.css? -
DIRECT/199.93.36.254 -
1383659364.906    250 192.168.2.5 TCP_REFRESH_HIT/304 327 GET
http://static2.playboy.com/assets/tour/js/vendor/jquery.unveil.min.js?
- DIRECT/8.254.10.253 -
1383659365.046    265 192.168.2.5 TCP_MISS/200 1524 GET
http://static2.playboy.com/assets/tour/img/newtour/blank.gif -
DIRECT/8.26.201.125 image/gif
1383659365.625   2813 192.168.2.3 TCP_MISS/200 338631 GET
http://admin.brightcove.com/viewer/us20131121.1403/federatedVideoUI/Br
ightcovePlayer.swf? - DIRECT/186.46.140.217 application/x-shockwave-
flash
1383659365.750    969 192.168.2.5 TCP_MISS/200 29460 GET
http://pictures.playboy.com/assets/content/photo/gallery/201311/14956/
images/264196/264196_thumb.jpg? - DIRECT/199.93.36.254 image/jpeg
1383659365.812   9422 192.168.2.3 TCP_MISS/200 604 GET
http://www.google.com.ec/ads/user-lists/991498594/? -
DIRECT/173.194.37.23 text/html
1383659365.859   1109 192.168.2.9 TCP_MISS/200 34017 GET
http://pictures.playboy.com/assets/content/photo/gallery/201311/14956/
images/264201/264201_thumb.jpg? - DIRECT/199.93.36.254 image/jpeg
1383659369.312   9375 192.168.2.3 TCP_MISS/200 3101 GET
http://admin.brightcove.com/viewer/us20131121.1403/BrightcoveBootloade
r.swf? - DIRECT/186.46.140.203 application/x-shockwave-flash
1383659369.500   4829 192.168.2.5 TCP_MISS/200 28098 GET
http://pictures.playboy.com/assets/content/photo/gallery/201311/14956/
images/264193/264193_thumb.jpg? - DIRECT/8.26.200.125 image/jpeg
1383659369.609   4906 192.168.2.5 TCP_MISS/200 80131 GET
http://ocsp.comodoca.com/ - DIRECT/178.255.83.1 application/ocsp-
response
1383659449.203    469 192.168.2.5 TCP_MISS/200 999 POST
http://ocsp.comodoca.com/ - DIRECT/178.255.83.1 application/ocsp-
response
1383659452.406    656 192.168.2.5 TCP_MISS/200 947 POST
http://ocsp.digicert.com/ - DIRECT/72.21.91.29 application/ocsp-
response
1383659452.984    438 192.168.2.5 TCP_MISS/200 947 POST
http://ocsp.digicert.com/ - DIRECT/72.21.91.29 application/ocsp-
response
1383659453.171  13750 192.168.2.5 TCP_MISS/200 59127 CONNECT dl-
debug17.dropbox.com:443 - DIRECT/107.20.249.71 -
1383659453.875    329 192.168.2.2 TCP_MISS/200 0 CONNECT
cdn.vendocdn.com:443 - DIRECT/174.35.22.81 -
1383659453.875    329 192.168.2.5 TCP_MISS/200 0 CONNECT
cdn.vendocdn.com:443 - DIRECT/174.35.10.194 -
1383659453.875   2813 192.168.2.5 TCP_MISS/200 28501 CONNECT
cdn.vendocdn.com:443 - DIRECT/174.35.22.81 -
```

```
1383659453.875    329 192.168.2.5 TCP_MISS/200 39 CONNECT
cdn.vendocdn.com:443 - DIRECT/174.35.10.194 -
1383659453.875    329 192.168.2.5 TCP_MISS/200 39 CONNECT
cdn.vendocdn.com:443 - DIRECT/174.35.10.194 -
1383659453.875    329 192.168.2.5 TCP_MISS/200 39 CONNECT
cdn.vendocdn.com:443 - DIRECT/174.35.22.81 -
1383659454.218    343 192.168.2.5 TCP_MISS/200 244 CONNECT
cdn.vendocdn.com:443 - DIRECT/174.35.22.81 -
1383659454.218    343 192.168.2.5 TCP_MISS/200 244 CONNECT
cdn.vendocdn.com:443 - DIRECT/174.35.10.194 -
1383659454.234    359 192.168.2.5 TCP_MISS/200 244 CONNECT
cdn.vendocdn.com:443 - DIRECT/174.35.10.194 -
1383659454.234    359 192.168.2.5 TCP_MISS/200 244 CONNECT
cdn.vendocdn.com:443 - DIRECT/174.35.22.81 -
1383659454.234    359 192.168.2.5 TCP_MISS/000 0 CONNECT
cdn.vendocdn.com:443 - NONE/- -
1383659454.984   1109 192.168.2.5 TCP_MISS/200 478 CONNECT
cdn.vendocdn.com:443 - DIRECT/174.35.22.81 -
1383659461.015  55875 192.168.2.5 TCP_MISS/200 301 GET
http://notify6.dropbox.com/subscribe? - DIRECT/108.160.163.42
text/plain
1383659463.093  60656 192.168.2.2 TCP_MISS/200 8179 CONNECT fbcdn-
photos-g-a.akamaihd.net:443 - DIRECT/23.0.163.35 -
1383659463.281 177266 192.168.2.5 TCP_MISS/200 28406 CONNECT
oauth.googleusercontent.com:443 - DIRECT/173.194.37.108 -
1383659463.296 181531 192.168.2.5 TCP_MISS/200 7446 CONNECT
accounts.google.com:443 - DIRECT/74.125.196.84 -
1383659463.671  21078 192.168.2.10 TCP_MISS/200 528 GET
http://realtime.services.disqus.com/api/2/thread/1984667586? -
DIRECT/184.173.90.195 application/json
1383659466.187    531 192.168.2.5 TCP_MISS/200 947 POST
http://ocsp.digicert.com/ - DIRECT/72.21.91.29 application/ocsp-
response
1383659466.234    453 192.168.2.5 TCP_MISS/200 934 POST
http://clients1.google.com/ocsp - DIRECT/173.194.37.3
application/ocsp-response
1383659466.562  13312 192.168.2.10 TCP_MISS/200 59911 CONNECT dl-
debug12.dropbox.com:443 - DIRECT/107.20.249.56 -
1383659466.984   1250 192.168.2.2 TCP_MISS/200 9145 CONNECT
lvs.xstreamjs.net:443 - DIRECT/75.126.114.66 -
1383659467.750    500 192.168.2.5 TCP_MISS/200 998 POST
http://ocsp.comodoca.com/ - DIRECT/178.255.83.1 application/ocsp-
response
1383659468.156    531 192.168.2.5 TCP_MISS/200 999 POST
http://ocsp.comodoca.com/ - DIRECT/178.255.83.1 application/ocsp-
response
1383659468.171   1484 192.168.2.5 TCP_MISS/200 9121 CONNECT
www.woopra.com:443 - DIRECT/108.168.218.164 -
```

```
1383659468.703    438 192.168.2.5 TCP_MISS/200 998 POST
http://ocsp.comodoca.com/ - DIRECT/178.255.83.1 application/ocsp-
response
1383659470.031  89469 192.168.2.5 TCP_MISS/200 4107 CONNECT fbstatic-
a.akamaihd.net:443 - DIRECT/186.46.140.208 -
1383659470.109  67656 192.168.2.5 TCP_MISS/200 10770 CONNECT fbcdn-
photos-a-a.akamaihd.net:443 - DIRECT/23.0.163.32 -
1383659471.171   4125 192.168.2.5 TCP_MISS/200 7959 CONNECT
i_rvzrjs_info.tlscdn.com:443 - DIRECT/198.7.58.218 -
1383659473.031  92469 192.168.2.5 TCP_MISS/200 10538 CONNECT fbstatic-
a.akamaihd.net:443 - DIRECT/186.46.140.211 -
1383659474.093  71656 192.168.2.5 TCP_MISS/200 7603 CONNECT fbcdn-
photos-c-a.akamaihd.net:443 - DIRECT/23.0.163.40 -
1383659474.312  27016 192.168.2.5 TCP_MISS/200 52271 CONNECT
secure3.vend-o.com:443 - DIRECT/93.188.253.193 -
1383659478.343    593 192.168.2.5 TCP_MISS/200 971 GET
http://www.xxx.com/ - DIRECT/141.0.173.173 text/html
1383659478.984  12297 192.168.2.5 TCP_MISS/200 60679 CONNECT dl-
debug4.dropbox.com:443 - DIRECT/107.20.249.241 -
1383659479.093     93 192.168.2.2 TCP_MISS/200 349 GET
http://186.42.193.235/pagead/ads.js? - DIRECT/186.42.193.235
application/x-javascript
1383659479.625    610 192.168.2.5 TCP_MISS/200 3883 GET
http://www.xxx.com/ - DIRECT/141.0.173.173 text/html
1383659479.828    860 192.168.2.5 TCP_MISS/200 3447 CONNECT
www.woopra.com:443 - DIRECT/108.168.218.168 -
1383659480.203    578 192.168.2.5 TCP_MISS/200 1609 GET
http://lvs.xstreamjs.net/amz/aeyJhZGRvbm5hbWUiOiJCb2J5THlyaWNzLTE1Iiwi
Y2xpZW50aWQiOiIxNDFlODNjNjAzNGZkZTAyZTM0YTUxMTVjYzlkNWRhYyIsImFmZmlkIj
oxMDYwLCJzdWJhZmZpZCI6MTA5MCwiaHJlZiI6Imh0dHA6Ly93d3cueHh4LmNvbS8iLCJ3
aWR0aCI6MTAyNCwiaGVpZ2h0Ijo2MDAsImxvYWRlcl9jbGllbnRfdGltZXN0YW1wIjoxMz
g1MTU4NTU0MDc3fQ%3D%3D.js - DIRECT/75.126.114.66 text/javascript
1383659480.656    266 192.168.2.5 TCP_MISS/200 594 GET
http://www.google-analytics.com/collect? - DIRECT/173.194.37.103
image/gif
1383659480.828    766 192.168.2.5 TCP_MISS/200 12147 GET
http://www.xxx.com/free-xxx-sex.gif - DIRECT/141.0.173.173 image/gif
1383659480.875    813 192.168.2.5 TCP_MISS/200 462 GET
http://www.xxx.com/xxx.gif - DIRECT/141.0.173.173 image/gif
1383659480.968    906 192.168.2.5 TCP_MISS/200 1219 GET
http://www.xxx.com/xxx_sex_2013.gif - DIRECT/141.0.173.173 image/gif
1383659481.390    937 192.168.2.5 TCP_MISS/200 479 GET
http://intext.nav-links.com/js/intext.js? - DIRECT/54.243.202.95
text/javascript
1383659481.734   1688 192.168.2.5 TCP_MISS/200 73931 GET
http://www.xxx.com/xxx-porn_video.gif - DIRECT/141.0.173.173 image/gif
1383659482.203   2141 192.168.2.5 TCP_MISS/200 71585 GET
http://www.xxx.com/xxx-sex-video.gif - DIRECT/141.0.173.173 image/gif
```

```
1383659483.859  16813 192.168.2.5 TCP_MISS/504 0 CONNECT intext.nav-
links.com:443 - DIRECT/54.243.169.117 -
1383659484.031  87297 192.168.2.5 TCP_MISS/200 31909 CONNECT fbstatic-
a.akamaihd.net:443 - DIRECT/186.46.140.208 -
1383659485.093  80906 192.168.2.5 TCP_MISS/200 3969 CONNECT fbcdn-
photos-c-a.akamaihd.net:443 - DIRECT/23.0.163.41 -
1383659485.093  82672 192.168.2.5 TCP_MISS/200 8163 CONNECT fbcdn-
photos-b-a.akamaihd.net:443 - DIRECT/23.0.163.27 -
1383659485.671   3093 192.168.2.5 TCP_MISS/404 410 GET
http://www.xxx.com/favicon.ico - DIRECT/141.0.173.173 text/html
1383659487.093  84672 192.168.2.5 TCP_MISS/200 7315 CONNECT fbcdn-
photos-h-a.akamaihd.net:443 - DIRECT/23.0.163.41 -
1383659488.031  91297 192.168.2.5 TCP_MISS/200 16523 CONNECT fbstatic-
a.akamaihd.net:443 - DIRECT/186.46.140.208 -
1383659488.781   9594 192.168.2.5 TCP_MISS/200 58711 CONNECT dl-
debug33.dropbox.com:443 - DIRECT/107.20.249.201 -
1383659491.031  94328 192.168.2.2 TCP_MISS/200 68654 CONNECT fbstatic-
a.akamaihd.net:443 - DIRECT/186.46.140.208 -
1383659491.437    672 192.168.2.5 TCP_MISS/200 3410 CONNECT
www.woopra.com:443 - DIRECT/108.168.218.175 -
1383659491.937  93672 192.168.2.5 TCP_MISS/200 535 GET
http://realtime.services.disqus.com/api/2/thread/1984667586? -
DIRECT/173.192.82.196 application/json
1383659492.546   3703 192.168.2.5 TCP_MISS/200 59015 CONNECT dl-
debug13.dropbox.com:443 - DIRECT/107.20.249.57 -
1383659495.031 114469 192.168.2.2 TCP_MISS/200 5898 CONNECT fbstatic-
a.akamaihd.net:443 - DIRECT/186.46.140.208 -
1383659496.171  35953 192.168.2.5 TCP_MISS/200 131355 CONNECT
cdn.vendocdn.com:443 - DIRECT/174.35.22.81 -
1383659496.171  35968 192.168.2.5 TCP_MISS/200 151362 CONNECT
cdn.vendocdn.com:443 - DIRECT/174.35.22.81 -
1383659496.359  36141 192.168.2.5 TCP_MISS/200 23095 CONNECT
cdn.vendocdn.com:443 - DIRECT/174.35.10.194 -
1383659497.093  89281 192.168.2.5 TCP_MISS/200 2161 CONNECT fbcdn-
photos-b-a.akamaihd.net:443 - DIRECT/23.0.163.27 -
1383659498.390  38172 192.168.2.5 TCP_MISS/200 26649 CONNECT
cdn.vendocdn.com:443 - DIRECT/174.35.10.194 -
1383659499.031 118453 192.168.2.5 TCP_MISS/200 10410 CONNECT fbstatic-
 secure3.vend-o.com:443 - DIRECT/93.188.253.193 -
1383659500.187  39969 192.168.2.5 TCP_MISS/200 476450 CONNECT
1383659512.031 131453 192.168.2.5 TCP_MISS/200 41211 CONNECT fbstatic-
a.akamaihd.net:443 - DIRECT/186.46.140.211 -
1383659513.031 110578 192.168.2.5 TCP_MISS/200 26899 CONNECT fbcdn-
profile-a.akamaihd.net:443 - DIRECT/186.46.140.211 -
1383659514.640   4672 192.168.2.5 TCP_MISS/200 59127 CONNECT dl-
debug9.dropbox.com:443 - DIRECT/107.20.249.252 -
1383659514.765 118031 192.168.2.2 TCP_MISS/200 32376 CONNECT fbstatic-
a.akamaihd.net:443 - DIRECT/186.46.140.208 -
```

```
1383659515.343    593 192.168.2.5 TCP_MISS/200 3447 CONNECT
www.woopra.com:443 - DIRECT/108.168.218.180 -
1383659516.640  55531 192.168.2.5 TCP_MISS/200 301 GET
http://notify6.dropbox.com/subscribe? - DIRECT/108.160.163.42
text/plain
1383659519.687   4969 192.168.2.2 TCP_MISS/200 58999 CONNECT dl-
debug10.dropbox.com:443 - DIRECT/107.20.250.7 -
1383659526.328   6563 192.168.2.2 TCP_MISS/200 59511 CONNECT dl-
debug2.dropbox.com:443 - DIRECT/107.20.249.37 -
1383659527.156    469 192.168.2.2 TCP_MISS/200 3447 CONNECT
www.woopra.com:443 - DIRECT/173.192.76.134 -
1383659532.484   6094 192.168.2.5 TCP_MISS/200 61367 CONNECT dl-
debug35.dropbox.com:443 - DIRECT/107.20.249.22 -
1383659535.031 206313 192.168.2.2 TCP_MISS/200 113906 CONNECT
fbstatic-a.akamaihd.net:443 - DIRECT/186.46.140.211 -
1383659539.406   6828 192.168.2.5 TCP_MISS/200 56359 CONNECT dl-
debug11.dropbox.com:443 - DIRECT/107.20.249.54 -
1383659540.093   1093 192.168.2.2 TCP_MISS/200 3447 CONNECT
www.woopra.com:443 - DIRECT/173.192.76.138 -
1383659542.031 210156 192.168.2.5 TCP_MISS/200 218966 CONNECT
fbstatic-a.akamaihd.net:443 - DIRECT/186.46.140.208 -
1383659544.562   5078 192.168.2.5 TCP_MISS/200 56695 CONNECT dl-
debug19.dropbox.com:443 - DIRECT/107.20.249.78 -
1383659550.734   6094 192.168.2.5 TCP_MISS/200 56295 CONNECT dl-
debug3.dropbox.com:443 - DIRECT/107.20.249.238 -
1383659551.437    766 192.168.2.2 TCP_MISS/200 3447 CONNECT
www.woopra.com:443 - DIRECT/173.193.174.194 -
1383659554.687 283562 192.168.2.5 TCP_MISS/200 130634 CONNECT
apis.google.com:443 - DIRECT/173.194.37.9 -
1383659559.171 273156 192.168.2.11 TCP_MISS/200 6253 CONNECT
ssl.gstatic.com:443 - DIRECT/173.194.37.15 -
1383659562.343  11547 192.168.2.5 TCP_MISS/200 56375 CONNECT dl-
debug38.dropbox.com:443 - DIRECT/107.20.249.221 -
1383659563.843   1109 192.168.2.2 TCP_MISS/200 3447 CONNECT
www.woopra.com:443 - DIRECT/108.168.218.164 -
1383659566.031 163610 192.168.2.5 TCP_MISS/200 30654 CONNECT fbcdn-
profile-a.akamaihd.net:443 - DIRECT/186.46.140.202 -
1383659568.187 165766 192.168.2.5 TCP_MISS/200 19436 CONNECT fbcdn-
profile-a.akamaihd.net:443 - DIRECT/186.46.140.200 -
1383659568.187 176281 192.168.2.5 TCP_MISS/200 54243 CONNECT fbcdn-
profile-a.akamaihd.net:443 - DIRECT/186.46.140.226 -
1383659568.187 165750 192.168.2.5 TCP_MISS/200 31191 CONNECT fbcdn-
profile-a.akamaihd.net:443 - DIRECT/186.46.140.210 -
1383659569.203 166782 192.168.2.5 TCP_MISS/200 14936 CONNECT fbcdn-
profile-a.akamaihd.net:443 - DIRECT/186.46.140.201 -
1383659570.421   8015 192.168.2.5 TCP_MISS/200 55959 CONNECT dl-
debug15.dropbox.com:443 - DIRECT/107.20.249.65 -
```

```
1383659572.984  56313 192.168.2.2 TCP_MISS/200 301 GET
http://notify6.dropbox.com/subscribe? - DIRECT/108.160.163.42
text/plain
1383659576.171   1500 192.168.2.2 TCP_MISS/200 3447 CONNECT
www.woopra.com:443 - DIRECT/108.168.218.168 -
1383659577.609   7125 192.168.2.5 TCP_MISS/200 57511 CONNECT dl-
debug31.dropbox.com:443 - DIRECT/107.20.249.190 -
1383659582.171 117671 192.168.2.2 TCP_MISS/200 13420 CONNECT
static.woopra.com:443 - DIRECT/72.21.91.19 -
1383659588.328  10641 192.168.2.5 TCP_MISS/200 56231 CONNECT dl-
debug27.dropbox.com:443 - DIRECT/107.20.249.148 -
1383659592.468   4093 192.168.2.2 TCP_MISS/200 56183 CONNECT dl-
debug26.dropbox.com:443 - DIRECT/107.20.249.139 -
1383659596.359   3828 192.168.2.2 TCP_MISS/200 6984 CONNECT dl-
debug30.dropbox.com:443 - DIRECT/107.20.249.164 -
1383659601.453    375 192.168.2.2 TCP_MISS/200 816 GET
http://cs.atdmt.com/? - DIRECT/31.13.73.1 image/gif
1383659601.515    422 192.168.2.5 TCP_MISS/200 816 GET
http://cs.atdmt.com/? - DIRECT/31.13.73.1 image/gif
1383659605.875   3532 192.168.2.5 TCP_MISS/200 972 GET
http://www.xnxx.com/ - DIRECT/141.0.174.39 text/html
1383659607.265     94 192.168.2.5 TCP_MISS/200 349 GET
http://186.42.193.235/pagead/ads.js? - DIRECT/186.42.193.235
application/x-javascript
1383659607.828  11407 192.168.2.5 TCP_MISS/200 56231 CONNECT dl-
debug17.dropbox.com:443 - DIRECT/107.20.249.71 -
1383659608.609   1469 192.168.2.2 TCP_MISS/200 60019 GET
http://www.xnxx.com/ - DIRECT/141.0.174.34 text/html
1383659608.937    781 192.168.2.5 TCP_MISS/200 11992 GET
http://static.xvideos.com/vote/displayFlash.js - DIRECT/141.0.172.252
application/x-javascript
1383659608.984    781 192.168.2.5 TCP_MISS/200 9594 GET
http://static.xvideos.com/js/mobile.js - DIRECT/141.0.172.252
application/x-javascript
1383659610.437   1203 192.168.2.5 TCP_MISS/200 14161 GET
http://img100.xvideos.com/xnxx.com/pics/xnxx.gif - DIRECT/68.142.118.4
image/gif
1383659610.796   1171 192.168.2.5 TCP_MISS/200 7847 GET
http://img100.xvideos.com/videos/thumbsl/07/9e/68/079e68e8544fcfc1f759
6fca08bdef00/079e68e8544fcfc1f7596fca08bdef00.21.jpg -
DIRECT/68.142.118.254 image/jpeg
1383659611.062   1406 192.168.2.5 TCP_MISS/200 13626 GET
http://img100.xvideos.com/videos/thumbsl/14/e7/45/14e745d6d15abbc96578
72bf45ac1f5d/14e745d6d15abbc9657872bf45ac1f5d.1.jpg -
DIRECT/68.142.118.4 image/jpeg
1383659611.250    625 192.168.2.5 TCP_MISS/200 10952 GET
http://img100.xvideos.com/videos/thumbsl/f0/22/3f/f0223fcdff9e4c912500
604737846dac/f0223fcdff9e4c912500604737846dac.15.jpg -
DIRECT/68.142.118.4 image/jpeg
```

```
1383659611.921    968 192.168.2.5 TCP_MISS/200 15808 GET
http://img100.xvideos.com/videos/thumbsl/28/48/7a/28487ad83402c2660921
a5f2629b1e09/28487ad83402c2660921a5f2629b1e09.25.jpg -
DIRECT/68.142.118.254 image/jpeg
1383659611.921    843 192.168.2.5 TCP_MISS/200 8641 GET
http://img100.xvideos.com/videos/thumbsl/7b/4d/79/7b4d79f42e72f2aa3296
d88521b3eeb8/7b4d79f42e72f2aa3296d88521b3eeb8.13.jpg -
DIRECT/68.142.118.4 image/jpeg
1383659611.921   1250 192.168.2.5 TCP_MISS/200 11070 GET
http://img100.xvideos.com/videos/thumbsl/bb/bb/67/bbbb67929d0c70f62529
8f41d375de80/bbbb67929d0c70f625298f41d375de80.16.jpg -
DIRECT/68.142.118.254 image/jpeg
1383659611.921   1250 192.168.2.5 TCP_MISS/200 10075 GET
http://img100.xvideos.com/videos/thumbsl/a8/d1/8c/a8d18c7c65dfee5f9609
1f21ee0ebee5/a8d18c7c65dfee5f96091f21ee0ebee5.26.jpg -
DIRECT/68.142.118.4 image/jpeg
1383659612.031   1328 192.168.2.5 TCP_MISS/200 10468 GET
http://img100.xvideos.com/videos/thumbsl/7b/2c/2d/7b2c2d7a7f5b346dc7ac
98c59fa77922/7b2c2d7a7f5b346dc7ac98c59fa77922.26.jpg -
DIRECT/68.142.118.4 image/jpeg
1383659612.046    828 192.168.2.5 TCP_MISS/200 2245 GET
http://static.xvideos.com/js/xnxx-ads.js? - DIRECT/141.0.172.252
application/x-javascript
1383659612.140   1422 192.168.2.5 TCP_MISS/200 9226 GET
http://img100.xvideos.com/videos/thumbsl/3a/48/b6/3a48b6dcd1e7357d9b3e
9d79399e604f/3a48b6dcd1e7357d9b3e9d79399e604f.13.jpg -
DIRECT/68.142.118.4 image/jpeg
1383659612.265   1281 192.168.2.5 TCP_MISS/200 11588 GET
http://img100.xvideos.com/videos/thumbsl/4e/db/c6/4edbc6c292680d44dc7e
c78e2127eaf1/4edbc6c292680d44dc7ec78e2127eaf1.19.jpg -
DIRECT/68.142.118.4 image/jpeg
1383659612.328   1625 192.168.2.5 TCP_MISS/200 14126 GET
http://img100.xvideos.com/videos/thumbsl/a5/dc/f6/a5dcf674cbe8921bd6fa
5c7c333e6ab5/a5dcf674cbe8921bd6fa5c7c333e6ab5.25.jpg -
DIRECT/68.142.118.254 image/jpeg
1383659612.937   1953 192.168.2.5 TCP_MISS/200 12047 GET
http://img100.xvideos.com/videos/thumbsl/04/b6/aa/04b6aaa2b5cda36eaa7b
ee480e06695f/04b6aaa2b5cda36eaa7bee480e06695f.13.jpg -
DIRECT/68.142.118.254 image/jpeg
1383659612.937   1937 192.168.2.5 TCP_MISS/200 11888 GET
http://img100.xvideos.com/videos/thumbsl/0b/a9/31/0ba931c7e988b5c7c1f9
19c5e1997974/0ba931c7e988b5c7c1f919c5e1997974.2.jpg -
DIRECT/68.142.118.4 image/jpeg
1383659612.953   1953 192.168.2.5 TCP_MISS/200 12150 GET
http://img100.xvideos.com/videos/thumbsl/a9/41/c7/a941c70e6636639b539d
2d1acde23616/a941c70e6636639b539d2d1acde23616.22.jpg -
DIRECT/68.142.118.254 image/jpeg
1383659613.203    188 192.168.2.5 TCP_MISS/200 12506 GET
```

```
http://img100.xvideos.com/xnxx.com/pics/xnb.gif -
DIRECT/68.142.118.254 image/gif
1383659615.187   2844 192.168.2.5 TCP_MISS/200 9207 GET
http://img100.xvideos.com/videos/thumbsl/07/62/7b/07627b078cdd47a8ac22
926fa8163beb/07627b078cdd47a8ac22926fa8163beb.16.jpg -
DIRECT/68.142.118.4 image/jpeg
1383659615.234   4219 192.168.2.5 TCP_MISS/200 10515 GET
http://img100.xvideos.com/videos/thumbsl/39/ad/72/39ad729065ec6f9193db
6f8dd68a783a/39ad729065ec6f9193db6f8dd68a783a.24.jpg -
DIRECT/68.142.118.4 image/jpeg
1383659615.265   7281 192.168.2.5 TCP_MISS/200 57047 CONNECT dl-
debug12.dropbox.com:443 - DIRECT/107.20.249.56 -
1383659615.671   4578 192.168.2.5 TCP_MISS/200 9052 GET
http://img100.xvideos.com/videos/thumbsl/7d/6f/f8/7d6ff85856df1f64d2dd
4fc36a046c7e/7d6ff85856df1f64d2dd4fc36a046c7e.27.jpg -
DIRECT/68.142.118.254 image/jpeg
1383659615.953   3782 192.168.2.5 TCP_MISS/200 369 GET
http://www.xnxx.com/ih.php? - DIRECT/141.0.174.35 text/html
1383659616.296   5281 192.168.2.5 TCP_MISS/200 15524 GET
http://img100.xvideos.com/videos/thumbsl/21/d1/4d/21d14d70d9fb2deac565
e4a5c35a735c/21d14d70d9fb2deac565e4a5c35a735c.9.jpg -
DIRECT/68.142.118.4 image/jpeg
1383659616.484   2813 192.168.2.5 TCP_MISS/200 7681 GET
http://img.xnxx.com/images/THUMBNAILS/240x180/971/971959/1.jpg -
DIRECT/68.142.118.4 image/jpeg
1383659616.890    250 192.168.2.5 TCP_MISS/200 6209 GET
http://img100.xvideos.com/videos/thumbs/f0/3a/f2/f03af20e036d0f014c008
a0a93dbe27c/f03af20e036d0f014c008a0a93dbe27c.16.jpg -
DIRECT/68.142.118.254 image/jpeg
1383659617.000   5985 192.168.2.5 TCP_MISS/200 14684 GET
http://img100.xvideos.com/videos/thumbsl/49/55/0b/49550ba8dae90310111d
444f8f80fa24/49550ba8dae90310111d444f8f80fa24.16.jpg -
DIRECT/68.142.118.254 image/jpeg
1383659617.062   6422 192.168.2.5 TCP_MISS/200 9700 GET
http://img100.xvideos.com/videos/thumbsl/39/59/7e/39597e461984ccac7940
08536e602662/39597e461984ccac794008536e602662.9.jpg -
DIRECT/68.142.118.4 image/jpeg
1383659617.078   5985 192.168.2.5 TCP_MISS/200 11925 GET
http://img100.xvideos.com/videos/thumbsl/01/54/f5/0154f522528eed76e953
85d9747844fe/0154f522528eed76e95385d9747844fe.18.jpg -
DIRECT/68.142.118.254 image/jpeg
1383659617.093    218 192.168.2.5 TCP_MISS/200 3694 GET
http://img100.xvideos.com/videos/thumbs/be/39/4d/be394d10572f2dac5964f
66d5457a587/be394d10572f2dac5964f66d5457a587.19.jpg -
DIRECT/68.142.118.254 image/jpeg
1383659617.109   5750 192.168.2.5 TCP_MISS/200 3147 GET
http://s7.addthis.com/js/250/addthis_widget.js - DIRECT/72.21.91.196
application/x-javascript
```

```
1383659617.125   3297 192.168.2.5 TCP_MISS/200 7396 GET
http://img.xnxx.com/images/THUMBNAILS/240x180/969/969935/1.jpg -
DIRECT/68.142.118.254 image/jpeg
1383659617.796    375 192.168.2.5 TCP_MISS/200 9360 GET
http://www.xxx.com/ - DIRECT/141.0.173.173 text/html
1383659799.781      0 192.168.2.3 TCP_MEM_HIT/200 470 GET
http://www.xxx.com/xxx.gif - NONE/- image/gif
1383659799.968      0 192.168.2.3 TCP_HIT/200 12155 GET
http://www.xxx.com/free-xxx-sex.gif - NONE/- image/gif
1383659799.968      0 192.168.2.3 TCP_MEM_HIT/200 1227 GET
http://www.google-analytics.com/analytics.js - DIRECT/173.194.37.7
text/javascript
1383659800.265 335640 192.168.2.5 TCP_MISS/200 28745 CONNECT
ssl.google-analytics.com:443 - DIRECT/173.194.37.126 -
1383659801.250 177344 192.168.2.5 TCP_MISS/200 1862 CONNECT
ssl.gstatic.com:443 - DIRECT/173.194.37.15 -
1383659801.437   5375 192.168.2.5 TCP_MISS/200 59479 CONNECT dl-
debug3.dropbox.com:443 - DIRECT/107.20.249.238 -
1383659801.750    110 192.168.2.2 TCP_MISS/200 594 GET
http://www.google-analytics.com/collect? - DIRECT/173.194.37.7
image/gif
1383659802.234    219 192.168.2.3 TCP_MISS/404 409 GET
http://www.xxx.com/favicon.ico - DIRECT/141.0.173.173 text/html
1383659802.328      0 192.168.2.3 TCP_NEGATIVE_HIT/404 408 GET
http://www.xxx.com/favicon.ico - NONE/- text/html
1383659807.687   6172 192.168.2.5 TCP_MISS/200 80338 CONNECT dl-
debug38.dropbox.com:443 - DIRECT/107.20.249.221 -
1383659817.000   9235 192.168.2.2 TCP_MISS/200 67591 CONNECT dl-
debug15.dropbox.com:443 - DIRECT/107.20.249.65 -
1383659819.234  56844 192.168.2.2 TCP_MISS/200 301 GET
http://notify6.dropbox.com/subscribe? - DIRECT/108.160.163.42
text/plain
1383659822.890   5828 192.168.2.2 TCP_MISS/200 65399 CONNECT dl-
debug31.dropbox.com:443 - DIRECT/107.20.249.190 -
1383659828.015   5047 192.168.2.2 TCP_MISS/200 65015 CONNECT dl-
debug27.dropbox.com:443 - DIRECT/107.20.249.148 -
1383659834.000   5938 192.168.2.2 TCP_MISS/200 61207 CONNECT dl-
debug26.dropbox.com:443 - DIRECT/107.20.249.139 -
1383659842.203    235 192.168.2.3 TCP_MISS/504 1522 GET
http://aflecha.net/archivo/tags/porno - DIRECT/aflecha.net text/html
1383659842.906   8860 192.168.2.5 TCP_MISS/200 65463 CONNECT dl-
debug30.dropbox.com:443 - DIRECT/107.20.249.164 -
1383659843.343      0 192.168.2.2 TCP_MISS/504 1508 GET
http://aflecha.net/favicon.ico - DIRECT/aflecha.net text/html
1383659843.531      0 192.168.2.3 TCP_MISS/504 1508 GET
http://aflecha.net/favicon.ico - DIRECT/aflecha.net text/html
http://laflecha.net/archivo/cache/thumbnails/i/50x50/storage/news/0047
/686_85933__xxx.jpg - DIRECT/70.32.99.26 image/jpeg
```

1383659866.765   1531 192.168.2.3 TCP_MISS/200 1631 GET
http://laflecha.net/archivo/cache/thumbnails/i/50x50/storage/news/0062
/310_uk-porn-websites.jpg - DIRECT/70.32.99.26 image/jpeg
1383659867.500   157 192.168.2.3 TCP_MISS/200 1999 GET
http://laflecha.net/archivo/cache/thumbnails/i/50x50/storage/news/0045
/688_playboyipad.jpg - DIRECT/70.32.99.26 image/jpeg
1383659867.640   3312 192.168.2.3 TCP_MISS/301 795 GET
http://laflecha.net/cache/thumbnails/i/50x50/storage/news/0020/957_sex
9.jpg - DIRECT/70.32.99.26 text/html
1383659867.703   3344 192.168.2.3 TCP_MISS/301 808 GET
http://laflecha.net/cache/thumbnails/i/50x50/storage/news/0016/823_por
no-pizza.jpg - DIRECT/70.32.99.26 text/html
1383659867.718   3390 192.168.2.3 TCP_MISS/301 795 GET
http://laflecha.net/cache/thumbnails/i/50x50/storage/news/0021/764_pc3
6.jpg - DIRECT/70.32.99.26 text/html
1383659867.734   3391 192.168.2.3 TCP_MISS/301 805 GET
http://laflecha.net/cache/thumbnails/i/50x50/storage/news/0018/653_sil
houette.jpg - DIRECT/70.32.99.26 text/html
1383659867.765   156 192.168.2.3 TCP_MISS/200 2711 GET
http://laflecha.net/archivo/cache/thumbnails/i/50x50/storage/news/0045
/528_porn.jpg - DIRECT/70.32.99.26 image/jpeg
1383659867.921   156 192.168.2.3 TCP_MISS/200 2053 GET
http://laflecha.net/archivo/cache/thumbnails/i/50x50/storage/news/0045
/479_marge.jpg - DIRECT/70.32.99.26 image/jpeg
1383659867.968   3640 192.168.2.3 TCP_MISS/301 795 GET
http://laflecha.net/cache/thumbnails/i/50x50/storage/news/0021/361_sex
6.jpg - DIRECT/70.32.99.26 text/html
1383659868.015   156 192.168.2.3 TCP_MISS/200 2004 GET
http://laflecha.net/archivo/cache/thumbnails/i/50x50/storage/news/0044
/236_porno_3d-595x409.jpg - DIRECT/70.32.99.26 image/jpeg
1383659868.031   172 192.168.2.3 TCP_MISS/200 1957 GET
http://laflecha.net/archivo/cache/thumbnails/i/50x50/storage/news/0041
/719_yaela.jpg - DIRECT/70.32.99.26 image/jpeg
1383659868.109   156 192.168.2.3 TCP_MISS/200 1572 GET
http://laflecha.net/archivo/cache/thumbnails/i/50x50/storage/news/0041
/013_bolis.jpg - DIRECT/70.32.99.26 image/jpeg
1383659868.171   156 192.168.2.3 TCP_MISS/200 2343 GET
http://laflecha.net/archivo/cache/thumbnails/i/50x50/storage/news/0039
/766_imagen.jpg - DIRECT/70.32.99.26 image/jpeg
1383659868.250   157 192.168.2.3 TCP_MISS/200 2864 GET
http://laflecha.net/archivo/cache/thumbnails/i/50x50/storage/news/0038
/418_sex.jpg - DIRECT/70.32.99.26 image/jpeg
1383659868.437   281 192.168.2.3 TCP_MISS/200 1938 GET
http://s2.juegosfriv.com/wp-content/themes/wpfriv/images/btn_home.png
- DIRECT/198.178.126.240 image/png
1383660525.468   265 192.168.2.1 TCP_MISS/200 4148 GET
http://s2.juegosfriv.com/wp-content/themes/wpfriv/images/btn_back.png
- DIRECT/198.178.126.240 image/png

```
1383660525.515    312 192.168.2.1 TCP_MISS/200 11672 GET
http://s3.juegosfriv.com/wp-
content/themes/wpfriv/images/xenobras.png.pagespeed.ic.vsUG7MdnIJ.jpg
- DIRECT/198.178.126.240 image/jpeg
1383660525.531    328 192.168.2.1 TCP_MISS/200 1999 GET
http://s2.juegosfriv.com/wp-content/uploads/thumbs/56x55xtop-unas-con-
kristen-stewart.jpg.pagespeed.ic.OuX93fk8b5.jpg -
DIRECT/198.178.126.240 image/jpeg
1383660525.546    343 192.168.2.1 TCP_MISS/200 1816 GET
http://s3.juegosfriv.com/wp-content/uploads/thumbs/56x55xladron-de-
conejo.jpg.pagespeed.ic.BWOcsTGzt2.jpg - DIRECT/198.178.126.240
image/jpeg
1383660525.546    328 192.168.2.1 TCP_MISS/200 2285 GET
http://s1.juegosfriv.com/wp-content/uploads/thumbs/56x55xdiscoteca-
coquetear.jpg.pagespeed.ic.aMeLQTwNGA.jpg - DIRECT/198.178.126.240
image/jpeg
1383660525.562    344 192.168.2.1 TCP_MISS/200 2291 GET
http://s3.juegosfriv.com/wp-
content/uploads/thumbs/56x55xgallinero.jpg.pagespeed.ic.gut9Gtgr9U.jpg
- DIRECT/198.178.126.240 image/jpeg
1383660525.578    360 192.168.2.1 TCP_MISS/200 1661 GET
http://s4.juegosfriv.com/wp-
content/uploads/thumbs/56x55xIQtest.jpg.pagespeed.ic.7hDKqsXOND.jpg -
DIRECT/198.178.126.240 image/jpeg
1383660525.593    375 192.168.2.1 TCP_MISS/200 2153 GET
http://s4.juegosfriv.com/wp-content/uploads/thumbs/56x55xtom-y-jerry-
rig-el-bridge1.jpg.pagespeed.ic.YVydgNcm5a.jpg -
DIRECT/198.178.126.240 image/jpeg
1383660525.609    391 192.168.2.1 TCP_MISS/200 2155 GET
http://s2.juegosfriv.com/wp-content/uploads/thumbs/56x55xunas-taller-
del-color.jpg.pagespeed.ic.t4JujaapS2.jpg - DIRECT/198.178.126.240
image/jpeg
1383660525.812    141 192.168.2.1 TCP_MISS/200 8172 GET
http://s2.juegosfriv.com/wp-content/themes/wpfriv/js/css-
pop.js,Mjm.EPBTU1w_gN.js+jscroller2-
1.61.js,Mjm.OEDrKk7KCK.js.pagespeed.jc.YFGXnmNcrD.js -
DIRECT/198.178.126.240 application/javascript
1383660526.203    594 192.168.2.1 TCP_MISS/200 16849 GET
http://s1.juegosfriv.com/wp-
content/themes/wpfriv/images/xbtn_play_another_game.png.pagespeed.ic.s
MGGlACUDC.png - DIRECT/198.178.126.240 image/png
1383660529.796   4125 192.168.2.1 TCP_MISS/200 268881 GET
http://code.jquery.com/jquery-1.9.1.js - DIRECT/108.161.188.209
application/x-javascript
1383660529.843   4172 192.168.2.1 TCP_MISS/200 52041 GET
http://ajax.googleapis.com/ajax/libs/jqueryui/1.8.0/jquery-ui.min.js -
DIRECT/74.125.196.95 text/javascript
1383660530.046   4375 192.168.2.1 TCP_MISS/200 145222 GET
http://s2.juegosfriv.com/wp-content/themes/wpfriv/js/jquery-
```

```
1.9.1.js.pagespeed.jm.It7AQ2eLvN.js - DIRECT/198.178.126.240
application/x-javascript
1383660530.078   4407 192.168.2.1 TCP_MISS/200 33460 GET
http://ajax.googleapis.com/ajax/libs/jquery/1/jquery.min.js -
DIRECT/74.125.196.95 text/javascript
1383660530.515    390 192.168.2.1 TCP_MISS/200 5685 GET
http://static.getclicky.com/js - DIRECT/190.93.246.10 application/x-
javascript
1383660530.515    359 192.168.2.1 TCP_MISS/200 6610 GET
http://googleads.g.doubleclick.net/pagead/html/r20131120/r20130906/zrt
_lookup.html - DIRECT/173.194.37.13 text/html
1383660530.812    609 192.168.2.1 TCP_MISS/200 44623 GET
http://pagead2.googlesyndication.com/pagead/expansion_embed.js -
DIRECT/173.194.37.26 text/javascript
1383660531.125    500 192.168.2.1 TCP_MISS/200 617 GET
http://in.getclicky.com/in.php? - DIRECT/198.145.13.22 text/javascript
1383660531.312    437 192.168.2.1 TCP_MISS/200 9353 GET
http://googleads.g.doubleclick.net/pagead/ads? - DIRECT/173.194.37.13
text/html
1383660531.562    281 192.168.2.1 TCP_MISS/200 32129 GET
http://pagead2.googlesyndication.com/simgad/4112357004212372669 -
DIRECT/173.194.37.26 image/jpeg
1383660531.609    609 192.168.2.1 TCP_MISS/200 9384 GET
http://googleads.g.doubleclick.net/pagead/ads? - DIRECT/173.194.37.25
text/html
1383660531.718    609 192.168.2.1 TCP_MISS/200 9373 GET
http://googleads.g.doubleclick.net/pagead/ads? - DIRECT/173.194.37.26
text/html
1383660532.031    453 192.168.2.1 TCP_MISS/200 50161 GET
http://pagead2.googlesyndication.com/simgad/13621896698824087145 -
DIRECT/173.194.37.26 image/jpeg
1383660532.046    406 192.168.2.1 TCP_MISS/200 1984 GET
http://s3.juegosfriv.com/wp-content/uploads/masqueradeballparty.swf -
DIRECT/198.178.126.240 application/x-shockwave-flash
1383660535.359    547 192.168.2.1 TCP_MISS/200 2325 POST
http://ocsp.verisign.com/ - DIRECT/199.7.71.72 application/ocsp-
response
1383660543.937  55328 192.168.2.5 TCP_MISS/200 301 GET
http://notify6.dropbox.com/subscribe? - DIRECT/108.160.163.42
text/plain
1383660544.968    453 192.168.2.1 TCP_MISS/200 3883 GET
http://www.xxx.com/ - DIRECT/141.0.173.173 text/html
1383660545.000      0 192.168.2.1 TCP_MEM_HIT/200 1228 GET
http://www.xxx.com/xxx_sex_2013.gif - NONE/- image/gif
1383660545.000      0 192.168.2.1 TCP_MEM_HIT/200 471 GET
http://www.xxx.com/xxx.gif - NONE/- image/gif
1383660545.000      0 192.168.2.1 TCP_HIT/200 12156 GET
http://www.xxx.com/free-xxx-sex.gif - NONE/- image/gif
1383660545.000      0 192.168.2.1 TCP_HIT/200 73940 GET
```

```
http://media.trafficfactory.biz//banners/1/be87b514228def49.jpg -
DIRECT/68.142.118.254 image/jpeg
1383660562.484   1406 192.168.2.5 TCP_MISS/200 174225 GET
http://media.trafficfactory.biz//banners/88/859b12369c1b8c5b4f1ac10197
632c0f.jpg - DIRECT/68.142.118.4 image/jpeg
1383660564.796    484 192.168.2.5 TCP_MISS/200 34361 GET
http://img100.xvideos.com/videos/thumbslll/be/eb/b3/beebb368416a2e6b07
e20859eec34eca/beebb368416a2e6b07e20859eec34eca.3.jpg -
DIRECT/68.142.118.4 image/jpeg
1383660566.078    282 192.168.2.5 TCP_MISS/200 423 GET
http://m.addthis.com/live/red_lojson/300lo.json? -
DIRECT/64.215.255.64 application/javascript
1383660570.390 180734 192.168.2.5 TCP_MISS/200 8001 CONNECT
pixel.facebook.com:443 - DIRECT/31.13.73.1 -
1383660583.031  46422 192.168.2.1 TCP_MISS/200 33013 CONNECT fbstatic-
a.akamaihd.net:443 - DIRECT/186.46.140.219 -
1383660583.031  47156 192.168.2.1 TCP_MISS/200 60793 CONNECT fbstatic-
a.akamaihd.net:443 - DIRECT/186.46.140.219 -
1383660588.906 158469 192.168.2.5 TCP_MISS/200 5044 CONNECT
186.226.233.54:443 - DIRECT/186.226.233.54 -
1383660590.984    359 192.168.2.1 TCP_MISS/200 540 GET
http://in.getclicky.com/in.php? - DIRECT/198.145.13.24 text/javascript
1383660593.031  56422 192.168.2.1 TCP_MISS/200 4522 CONNECT fbstatic-
a.akamaihd.net:443 - DIRECT/186.46.140.219 -
1383660599.250  55235 192.168.2.5 TCP_MISS/200 301 GET
http://notify6.dropbox.com/subscribe? - DIRECT/108.160.163.42
text/plain
1383660601.031  65156 192.168.2.2 TCP_MISS/200 3450 CONNECT fbstatic-
a.akamaihd.net:443 - DIRECT/186.46.140.211 -
1383660607.750     16 192.168.2.1 TCP_HIT/200 23965 GET
http://legalporno.com/assets/css/jquery-ui-custom.css - NONE/-
text/css
1383660607.750     16 192.168.2.1 TCP_HIT/200 34039 GET
http://ajax.googleapis.com/ajax/libs/jquery/1.8.2/jquery.min.js -
NONE/- text/javascript
1383660607.750     16 192.168.2.1 TCP_HIT/200 63110 GET
http://ajax.googleapis.com/ajax/libs/jqueryui/1.9.1/jquery-ui.min.js -
NONE/- text/javascript
1383660608.171    421 192.168.2.1 TCP_REFRESH_HIT/200 5565 GET
http://legalporno.com/skins/legalporn/css/dialogs.css? -
DIRECT/141.0.175.110 text/css
1383660608.203    453 192.168.2.1 TCP_REFRESH_HIT/200 33623 GET
http://legalporno.com/skins/legalporn/css/dlx-css.css? -
DIRECT/141.0.175.110 text/css
1383660608.234    484 192.168.2.1 TCP_REFRESH_HIT/200 6906 GET
http://legalporno.com/skins/legalporn/css/thumbnails.css? -
DIRECT/141.0.175.110 text/css
1383660608.265    515 192.168.2.1 TCP_REFRESH_HIT/200 6272 GET
```

```
http://legalporno.com/assets/js/auth.js? - DIRECT/141.0.175.110
application/x-javascript
1383660608.734    984 192.168.2.1 TCP_REFRESH_HIT/200 1317 GET
http://assets-nl.gtflix.com/js/models/AuthRequiringModel.js? -
DIRECT/141.0.175.110 application/x-javascript
1383660608.750   1000 192.168.2.1 TCP_REFRESH_HIT/200 1103 GET
http://legalporno.com/assets/js/subscribe.js? - DIRECT/141.0.175.110
application/x-javascript
1383660608.843   1093 192.168.2.1 TCP_REFRESH_HIT/200 858 GET
http://legalporno.com/assets/js/search.js? - DIRECT/141.0.175.110
application/x-javascript
1383660608.843   1093 192.168.2.1 TCP_REFRESH_HIT/200 16016 GET
http://legalporno.com/assets/js/plugin/jquery.jcarousel.min.js? -
DIRECT/141.0.175.110 application/x-javascript
1383660608.859   1109 192.168.2.1 TCP_REFRESH_HIT/200 2531 GET
http://legalporno.com/assets/images/header/smart-but_02.png - NONE/-
image/png
1383660609.265      0 192.168.2.1 TCP_MEM_HIT/200 1534 GET
http://legalporno.com/skins/legalporn/images/filter/filter-bg2.png -
NONE/- image/png
1383660609.296      0 192.168.2.1 TCP_HIT/200 8667 GET
http://cdn4.nl.gtflix.com/dl/a2d56192836163bbd66cc9ebd61fe35a/D/1/14/1
348/3/sz304x171c/081.jpg - NONE/- image/jpeg
1383660609.390    125 192.168.2.1 TCP_MISS/200 562 GET
http://www.google-analytics.com/__utm.gif? - DIRECT/173.194.37.99
image/gif
1383660609.453      0 192.168.2.1 TCP_HIT/200 8414 GET
http://cdn2.nl.gtflix.com/dl/388d9cb67d8aeab415392da81c409907/D/1/14/1
108/3/sz304x171c/039.jpg - NONE/- image/jpeg
1383660609.531     16 192.168.2.1 TCP_HIT/200 9637 GET
http://cdn3.nl.gtflix.com/dl/e478c6d3329d8f78c05b7a2e5865dca2/D/1/14/1
230/3/sz304x171c/062.jpg - NONE/- image/jpeg
1383660609.546    265 192.168.2.1 TCP_REFRESH_HIT/200 58832 GET
http://connect.facebook.net/en_US/all.js - DIRECT/23.5.159.139
application/x-javascript
1383660609.593      0 192.168.2.1 TCP_HIT/200 10518 GET
http://static.ak.facebook.com/connect/xd_arbiter.php? - NONE/-
text/html
1383660609.640    437 192.168.2.1 TCP_REFRESH_HIT/200 6837 GET
http://cdn3.nl.gtflix.com/dl/a7b336550b7eba6157a73fbdb75059c0/D/1/15/2
81/3/sz304x171c/045.jpg - DIRECT/141.0.175.79 image/jpeg
1383660611.140      0 192.168.2.1 TCP_HIT/200 26780 GET
http://platform.twitter.com/widgets/tweet_button.1384994725.html -
NONE/- text/html
1383660611.140      0 192.168.2.1 TCP_HIT/200 29556 GET
http://platform.twitter.com/widgets/follow_button.1384994725.html -
NONE/- text/html
```

```
1383660611.187     47 192.168.2.1 TCP_MISS/200 990 GET
http://legalporno.com/filter/initialize - DIRECT/141.0.175.110
text/html
1383660611.468    281 192.168.2.1 TCP_MISS/200 654 GET
http://p.twitter.com/f.gif? - DIRECT/23.7.113.224 image/gif
1383660611.500    313 192.168.2.1 TCP_MISS/200 654 GET
http://p.twitter.com/t.gif? - DIRECT/23.7.113.224 image/gif
1383660611.609    313 192.168.2.1 TCP_REFRESH_MISS/200 584 GET
http://cdn.api.twitter.com/1/urls/count.json? - DIRECT/23.7.113.224
application/javascript
1383660612.156    610 192.168.2.1 TCP_MISS/200 2360 POST
http://evsecure-ocsp.verisign.com/ - DIRECT/199.7.57.72
application/ocsp-response
1383660612.156      0 192.168.2.1 TCP_MEM_HIT/200 950 GET
http://evsecure-crl.verisign.com/pca3-g5.crl - NONE/-
application/pkix-crl
1383660612.265   1125 192.168.2.1 TCP_MISS/200 7179 GET
http://www.facebook.com/plugins/like.php? - DIRECT/31.13.73.1
text/html
1383660612.265      0 192.168.2.1 TCP_HIT/200 47025 GET
http://static.ak.fbcdn.net/rsrc.php/v2/yH/r/WgFL-tIhwUh.js - NONE/-
application/x-javascript
1383660612.734    578 192.168.2.1 TCP_MISS/200 2456 POST
http://evsecure-ocsp.verisign.com/ - DIRECT/199.7.57.72
application/ocsp-response
1383660612.984    250 192.168.2.1 TCP_REFRESH_HIT/200 80200 GET
http://evsecure-crl.verisign.com/EVSecure2006.crl - DIRECT/23.4.37.163
application/pkix-crl
1383660613.406    235 192.168.2.1 TCP_MISS/200 1505 GET
http://legalporno.com/favicon.ico - DIRECT/141.0.175.110 image/x-icon
1383660614.031  78156 192.168.2.1 TCP_MISS/200 54168 CONNECT fbstatic-
a.akamaihd.net:443 - DIRECT/186.46.140.203 -
1383660615.046   1171 192.168.2.1 TCP_MISS/200 110220 GET
http://cdn1.nl.gtflix.com/dl/58332ca94e1d2ccc16a692b6e6fb7d76/D/1/15/1
53/3/sz304x171c_tm009-013-017-029-032-035-036-037-051-058-068-075-076-
077-079-087/timeline.jpg - DIRECT/141.0.175.77 image/jpeg
1383660615.046  79359 192.168.2.1 TCP_MISS/200 70691 CONNECT fbstatic-
a.akamaihd.net:443 - DIRECT/186.46.140.203 -
1383660615.703   1844 192.168.2.1 TCP_MISS/200 558 POST
http://legalporno.com/track? - DIRECT/141.0.175.110 application/json
1383660629.281    625 192.168.2.1 TCP_MISS/200 2325 POST
http://ocsp.verisign.com/ - DIRECT/199.7.57.72 application/ocsp-
response
1383660629.296    609 192.168.2.1 TCP_MISS/200 2325 POST
http://ocsp.verisign.com/ - DIRECT/199.7.57.72 application/ocsp-
response
1383660629.546   1265 192.168.2.1 TCP_MISS/200 6055 CONNECT
services.addons.mozilla.org:443 - DIRECT/63.245.216.134 -
```

```
1383660630.140    594 192.168.2.1 TCP_MISS/200 1377 CONNECT
services.addons.mozilla.org:443 - DIRECT/63.245.216.134 -
1383660641.140  12906 192.168.2.1 TCP_MISS/200 7613 CONNECT
versioncheck-bg.addons.mozilla.org:443 - DIRECT/63.245.217.162 -
1383660643.187  32000 192.168.2.1 TCP_MISS/200 6915 CONNECT
twitter.com:443 - DIRECT/199.16.156.102 -
1383660650.203    235 192.168.2.1 TCP_REFRESH_HIT/304 292 GET
http://legalporno.com/skins/legalporn/css/dlx-css.css? -
DIRECT/141.0.175.110 -
1383660650.218    250 192.168.2.1 TCP_REFRESH_HIT/304 292 GET
http://assets-nl.gtflix.com/js/models/VideoModel.js? -
DIRECT/141.0.175.110 -
1383660650.250    282 192.168.2.1 TCP_REFRESH_HIT/304 292 GET
http://assets-nl.gtflix.com/js/models/AuthRequiringModel.js? -
DIRECT/141.0.175.110 -
1383660650.250    282 192.168.2.1 TCP_REFRESH_HIT/304 292 GET
http://assets-nl.gtflix.com/js/models/TrackModel.js? -
DIRECT/141.0.175.110 -
1383660650.281    313 192.168.2.1 TCP_REFRESH_HIT/304 292 GET
http://legalporno.com/assets/js/views/AuthStatusPanelView.js? -
DIRECT/141.0.175.110 -
1383660662.390    125 192.168.2.1 TCP_MISS/200 562 GET
http://www.google-analytics.com/__utm.gif? - DIRECT/173.194.37.99
image/gif
1383660662.562   2875 192.168.2.1 TCP_MISS/200 49479 GET
http://legalporno.com/model/model/id/463 - DIRECT/141.0.175.110
text/html
1383660662.718    531 192.168.2.1 TCP_MISS/200 7558 GET
http://cdn4.nl.gtflix.com/dl/b74745c3f60acaad3040d0f01213793c/D/1/9/31
5/3/sz304x171c/69.jpg - DIRECT/141.0.175.80 image/jpeg
1383660662.828    297 192.168.2.1 TCP_MISS/200 3829 GET
http://fonts.googleapis.com/css? - DIRECT/74.125.196.95 text/css
1383660667.265    390 192.168.2.1 TCP_MISS/200 665 GET
http://gamingwonderland.dl.tb.ask.com/favicon.ico -
DIRECT/74.113.233.180 image/x-icon
1383660667.406    172 192.168.2.1 TCP_MISS/200 1634 GET
http://ak.imgfarm.com/images/vicinio/dsp-
images/scott.schaffer/background/1369936989332.png -
DIRECT/186.46.140.226 image/png
1383660667.578    344 192.168.2.1 TCP_MISS/200 3996 GET
http://ak.imgfarm.com/images/download/ask/pba_0927.png -
DIRECT/186.46.140.219 image/png
1383660667.671    437 192.168.2.1 TCP_MISS/200 3525 GET
http://ak.imgfarm.com/images/download/runrun/test/rebuttal/Alert.png -
DIRECT/186.46.140.219 image/png
1383660668.031    797 192.168.2.1 TCP_MISS/200 15425 GET
http://ak.imgfarm.com/images/vicinio/dsp-
images/jason.pepping/asset3/1379342492439.png - DIRECT/186.46.140.226
image/png
```

```
1383660668.343   1109 192.168.2.1 TCP_MISS/302 1381 GET
http://segment-pixel.invitemedia.com/pixel? - DIRECT/108.170.192.199 -
1383660668.937   1687 192.168.2.1 TCP_MISS/200 22115 GET
http://themes.googleusercontent.com/static/fonts/roboto/v9/RxZJdnzeo3R
5zSexge8UUT8E0i7KZn-EPnyo3HZu7kw.woff - DIRECT/173.194.37.106
font/woff
1383660669.187    844 192.168.2.1 TCP_MISS/302 771 GET
http://ad.yieldmanager.com/pixel? - DIRECT/98.139.225.43 -
1383660669.296   2062 192.168.2.1 TCP_MISS/200 56789 GET
http://ak.imgfarm.com/images/vicinio/dsp-
images/jason.pepping/asset9/1384283317860.png - DIRECT/186.46.140.219
image/png
1383660669.421   2187 192.168.2.1 TCP_MISS/200 41995 GET
http://ak.imgfarm.com/images/anx/anemone-1.2.7.js -
DIRECT/186.46.140.226 application/javascript
1383660669.656    735 192.168.2.1 TCP_MISS/200 2065 POST
http://ocsp.verisign.com/ - DIRECT/199.7.57.72 application/ocsp-
response
1383660669.703   2469 192.168.2.1 TCP_MISS/302 1381 GET
http://segment-pixel.invitemedia.com/pixel? - DIRECT/108.170.192.199 -
1383660669.750   2516 192.168.2.1 TCP_MISS/200 56965 GET
http://ak.imgfarm.com/images/vicinio/dsp-
images/jason.pepping/asset12/1384283314144.png - DIRECT/186.46.140.226
image/png
1383660669.765    578 192.168.2.1 TCP_MISS/302 815 GET
http://ads.yahoo.com/pixel? - DIRECT/98.139.225.43 -
1383660670.140    437 192.168.2.1 TCP_MISS/302 771 GET
http://ad.yieldmanager.com/pixel? - DIRECT/98.139.225.42 -
1383660670.187   2953 192.168.2.1 TCP_MISS/200 283228 GET
http://ak.imgfarm.com/images/vicinio/dsp-
images/scott.schaffer/background999/1369937138915.jpg -
DIRECT/186.46.140.226 image/jpeg
1383660670.203    438 192.168.2.1 TCP_MISS/200 1323 GET
http://ads.yahoo.com/pixel? - DIRECT/98.139.225.42 image/gif
1383660670.468    328 192.168.2.1 TCP_MISS/200 1323 GET
http://ads.yahoo.com/pixel? - DIRECT/98.139.225.43 image/gif
1383660670.921    671 192.168.2.1 TCP_MISS/204 284 GET
http://free.gamingwonderland.com/anemone.jhtml? -
DIRECT/74.113.233.180 text/plain
1383660670.937    625 192.168.2.1 TCP_MISS/204 284 GET
http://free.gamingwonderland.com/anemone.jhtml? -
DIRECT/74.113.233.180 text/plain
1383660671.015    500 192.168.2.1 TCP_MISS/200 679 GET
http://3335366.fls.doubleclick.net/activityi;src=3335366;type=retar633
;cat=gwlre413;ord=1970474229115.8706 - DIRECT/173.194.37.28 text/html
1383660671.031    719 192.168.2.1 TCP_MISS/204 284 GET
http://free.gamingwonderland.com/anemone.jhtml? -
DIRECT/74.113.233.180 text/plain
```

```
1383660671.062   3828 192.168.2.1 TCP_MISS/302 844 GET
http://a.triggit.com/px? - DIRECT/63.131.141.170 text/html
1383660671.312    250 192.168.2.1 TCP_MISS/302 1138 GET
http://cm.g.doubleclick.net/pixel? - DIRECT/173.194.37.25 text/html
1383660671.468    156 192.168.2.1 TCP_MISS/302 667 GET
http://a.triggit.com/pxgcm? - DIRECT/63.131.141.170 text/html
1383660671.703    235 192.168.2.1 TCP_MISS/302 721 GET
http://www.facebook.com/fr/u.php? - DIRECT/31.13.73.1 text/html
1383660671.859    156 192.168.2.1 TCP_MISS/302 758 GET
http://a.triggit.com/pxfbcm? - DIRECT/63.131.141.170 text/html
1383660672.031    172 192.168.2.1 TCP_MISS/302 870 GET
http://tag.admeld.com/id? - DIRECT/186.46.140.201 text/html
1383660672.187    156 192.168.2.1 TCP_MISS/302 740 GET
http://a.triggit.com/pxamcm? - DIRECT/63.131.141.170 text/html
1383660672.468    281 192.168.2.1 TCP_MISS/302 835 GET
http://pixel.rubiconproject.com/tap.php? - DIRECT/69.25.24.24
text/html
1383660672.609    141 192.168.2.1 TCP_MISS/302 649 GET
http://a.triggit.com/pxruourcm - DIRECT/63.131.141.170 text/html
1383660672.953    344 192.168.2.1 TCP_MISS/302 500 GET
http://adadvisor.net/adscores/g.pixel? - DIRECT/216.120.27.21 -
1383660673.109    156 192.168.2.1 TCP_MISS/200 579 GET
http://a.triggit.com/pxtg? - DIRECT/63.131.141.170 image/gif
1383660700.218  32984 192.168.2.1 TCP_MISS/200 10586 CONNECT
seal.verisign.com:443 - DIRECT/199.7.55.231 -
1383660710.718  55672 192.168.2.5 TCP_MISS/200 301 GET
http://notify6.dropbox.com/subscribe? - DIRECT/108.160.163.42
text/plain
1383660725.859 116266 192.168.2.2 TCP_MISS/200 15023 CONNECT s-
static.ak.facebook.com:443 - DIRECT/23.5.146.110 -
1383660736.265 263750 192.168.2.5 TCP_MISS/200 45467 CONNECT
apis.google.com:443 - DIRECT/173.194.37.14 -
1383660738.296 262093 192.168.2.14 TCP_MISS/200 3086 CONNECT
ssl.gstatic.com:443 - DIRECT/173.194.37.15 -
1383660748.937    281 192.168.2.1 TCP_MISS/200 947 POST
http://ocsp.digicert.com/ - DIRECT/72.21.91.29 application/ocsp-
response
1383660749.187    234 192.168.2.1 TCP_MISS/200 965 GET
http://crl4.digicert.com/DigiCertHighAssuranceEVRootCA.crl -
DIRECT/204.93.142.142 application/x-pkcs7-crl
1383660749.468    281 192.168.2.1 TCP_MISS/200 1015 GET
http://crl3.digicert.com/DigiCertHighAssuranceEVRootCA.crl -
DIRECT/72.21.91.29 application/x-pkcs7-crl
1383660749.750    282 192.168.2.1 TCP_MISS/200 947 POST
http://ocsp.digicert.com/ - DIRECT/72.21.91.29 application/ocsp-
response
1383660749.859 115875 192.168.2.1 TCP_MISS/200 4230 CONNECT fbstatic-
a.akamaihd.net:443 - DIRECT/186.46.140.203 -
```

```
1383660749.906    141 192.168.2.1 TCP_MISS/200 7195 GET
http://crl4.digicert.com/evca1-g3.crl - DIRECT/204.93.142.142
application/x-pkcs7-crl
1383660750.078    172 192.168.2.1 TCP_MISS/200 7245 GET
http://crl3.digicert.com/evca1-g3.crl - DIRECT/72.21.91.29
application/x-pkcs7-crl
1383660766.656  55891 192.168.2.5 TCP_MISS/200 301 GET
http://notify6.dropbox.com/subscribe? - DIRECT/108.160.163.42
text/plain
1383660795.703    266 192.168.2.2 TCP_MISS/200 1142 POST
http://safebrowsing.clients.google.com/safebrowsing/downloads? -
DIRECT/173.194.37.3 application/vnd.google.safebrowsing-update
1383660796.000    282 192.168.2.14 TCP_MISS/200 5360 GET
http://safebrowsing-
cache.google.com/safebrowsing/rd/ChNnb29nLW1hbHdhcmUtc2hhdmFyEAEYmsoHI
J7KByoFHeUBAAMyBRrlAQAH - DIRECT/173.194.37.1
application/vnd.google.safebrowsing-chunk
1383660796.125    110 192.168.2.14 TCP_MISS/200 1025 GET
http://safebrowsing-
cache.google.com/safebrowsing/rd/ChNnb29nLW1hbHdhcmUtc2hhdmFyEAAYtfgHI
Mj4ByoHOPwBAP__ATIFNfwBAAc - DIRECT/173.194.37.1
application/vnd.google.safebrowsing-chunk
1383660796.250    125 192.168.2.15 TCP_MISS/200 2984 GET
http://safebrowsing-
cache.google.com/safebrowsing/rd/ChFnb29nLXBoaXNoLXNoYXZhchABGKGdCSDAn
gkqFbpOAgD_____________________fzIIoU4CAP___wE - DIRECT/173.194.37.1
application/vnd.google.safebrowsing-chunk
1383660796.406    141 192.168.2.15 TCP_MISS/200 5602 GET
http://notify6.dropbox.com/subscribe? - DIRECT/108.160.163.42
text/plain
1383660822.921    812 192.168.2.2 TCP_MISS/200 8857 CONNECT
lvs.xstreamjs.net:443 - DIRECT/75.126.223.162 -
1383660826.015  62484 192.168.2.5 TCP_MISS/200 1835 CONNECT fbstatic-
a.akamaihd.net:443 - DIRECT/186.46.140.211 -
1383660844.531    531 192.168.2.1 TCP_MISS/200 816 GET
http://cs.atdmt.com/? - DIRECT/31.13.73.1 image/gif
1383660848.343   5531 192.168.2.1 TCP_MISS/200 122936 GET
http://cdn3.nl.gtflix.com/dl/ac722f56cdf1b33e9dfd91f60d4f093e/D/1/11/1
061/3/sz304x171c_tm003-009-011-016-022-034-043-051-053-059-061-065-
086-091-092-095/timeline.jpg - DIRECT/141.0.175.79 image/jpeg
1383660851.218    234 192.168.2.1 TCP_MISS/200 2325 POST
http://ocsp.verisign.com/ - DIRECT/199.7.51.72 application/ocsp-
response
1383660851.234    641 192.168.2.1 TCP_MISS/200 4795 CONNECT 3-p-07-
ash2.channel.facebook.com:443 - DIRECT/173.252.113.17 -
1383660856.734    438 192.168.2.1 TCP_MISS/200 4748 CONNECT 3-p-07-
ash2.channel.facebook.com:443 - DIRECT/173.252.113.17 -
1383660857.140    390 192.168.2.1 TCP_MISS/200 4748 CONNECT 3-p-07-
ash2.channel.facebook.com:443 - DIRECT/173.252.113.17 -
```

```
1383660867.015    375 192.168.2.1 TCP_MISS/200 4775 CONNECT 3-p-07-
ash2.channel.facebook.com:443 - DIRECT/173.252.113.17 -
1383660867.406    391 192.168.2.1 TCP_MISS/200 4775 CONNECT 3-p-07-
ash2.channel.facebook.com:443 - DIRECT/173.252.113.17 -
1383660879.312   1172 192.168.2.1 TCP_MISS/200 1906 GET
http://pornbox.com/css/jquery.jscrollpane.css - DIRECT/141.0.175.55
text/css
1383660879.312   1172 192.168.2.1 TCP_MISS/200 5295 GET
```

Anexo 15: Incidencias de respaldos de log del servidor proxy

Se hace el seguimiento durante cinco días sobre los respaldos de log del servidor proxy teniendo la siguiente tabla:

Fecha	Incidencia	Descripción	Observación
10/10/2013	001	El log está vacío	Se solicita el respaldo pero, manifiesta el encargado de tecnología que eso maneja el profesor de Tics.
19/11/2013	002	El log está vacío	El profesor no tiene medios donde pueda respaldar ya que no le han proporcionado el CELP, y al reiniciar el computador se borra por el Freeze instalado.
20/11/2013	003	El log está vacío	No respalda nadie
21/11/2013	004	El log está vacío	No respalda nadie
22/11/2013	005	El log está vacío	No respalda nadie

Tabla A.8: Incidencias de respaldos de log del servidor proxy (Elaborado por: Investigador)

Anexo 16: Proforma de equipos de comunicaciones

OFERTA ECONÓMICA

Cliente: CENTRO EDUCATIVO LA PRADERA
Atención: ING. TANNIA MAYORGA
Dirección
Teléfono: 0983342785

MARTEL

Ref: CABLEADO ESTRUCTURADO
Fecha: 2013-11-25
Proyecto: 142
e-mail: tmayorga.sistemas@gmail.cc

ITEM	CÓDIGO	UND	DESCRIPCIÓN	CANT	P. UIO UNIT	PRECIO TOTAL	DISPONIBILIDAD
1	CIS SF300-24	UND	Cisco Smart Switch FE de 24-Port 10/100 + 2 Puertos (RJ-45 + SFP) combinados; 128 VLANs	2	224.70	449.40	
2	CIS SG500-28	UND	Cisco Switch Administrable Capa 3 de 24 Puertos 10/100/1000 + 2 Puertos GigE + 2 1GE/5GE SFP combinados; 4092 Vlans +	2	852.60	1,705.20	
3	CIS RV110W	UND	Cisco Router Wireless-N; 5 VPN firewall; 4 puertos LAN 10/100 + 1 WAN 10/100; 2 antenas integradas; 32 Usuarios; 2.4 GHz	2	101.85	203.70	
4	CIS WAP321-A-K9	UND	Cisco Access Point N 300 Mbps doble banda w/PoE + Portal Cautivo Hot Spot + Roaming Port 10/100/1000 cluster max 8 Aps	2	274.05	548.10	
					TOTAL	2,906.40	

CONDIICIONES COMERCIALES:
FORMA DE PAGO: A CONVENIR
TIEMPO DE ENTREGA: INMEDIATO UNA VEZ CONFIRMADO STOCK
VALIDEZ DE LA OFERTA: 8 DÍAS
- Estos precios no incluyen I.V.A.

Atentamente,

Tatiana Mosquera
VENTAS & INGENIERIA DE PROYECTOS
Juan Gonzalez N35-76 y Juan Pablo Sáinz
PBX: 2 225 1182 / 2155 Ext: 124
tmosquera@martel.com.ec
Movil: 0990435673

Anexo 17: Proforma de materiales

OFERTA ECONÓMICA

Cliente: CENTRO EDUCATIVO LA PRADERA
Atención: ING. TANNIA MAYORGA
Dirección
Teléfono: 0983342785

MARTEL CABLECOM

Ref: CABLEADO ESTRUCTURADO
Fecha: 2013-11-22
Proyecto: 141
e-mail: tmayorga.sistemas@gmail.cc

ITEM	CÓDIGO	UND	DESCRIPCIÓN	CANT	P. UIO UNIT	PRECIO TOTAL	DISPONIBILIDAD
1	BEA JPT-B42-E3GN	UND	RACK CERRADO 7'RP. 2000X600X800MM NEGRO PUERTA VIDRIO	1	931.90	931.90	INMEDIATO
2	BEA BNJ-101Y	UND	BANDEJA ESTANDAR 2Ur 19P. 89.5X444X367mm VENTILADA	1	17.10	17.10	INMEDIATO
3	BEA ORGV-58	UND	ORGANIZADOR VERTICAL SIMPLE 80X80 7:2	1	47.10	47.10	24 HORAS
4	BEA ORGH-43	UND	ORGANIZADOR HORIZONTAL CON CANALETA 60X80 19P.	2	15.43	30.86	INMEDIATO
5	LEV 5500-190	UND	REGLETA CORTAPICOS DE 12 PUERTOS P/RACK	2	196.11	392.22	INMEDIATO
6	LEV UTP5R-MLB	UND	Cable Cat. 5E CMR color Azul	1525	0.44	671.00	INMEDIATO
7	LEV 42080-2WS	UND	FACE PLATE DE 2 POSICIONES BLANCO	40	1.63	65.20	INMEDIATO
8	LEV 5G460-03W	UND	PATCH CORD CAT. 5E 3 FT. BLANCO	48	2.16	103.68	INMEDIATO
9	LEV 5G460-07W	UND	PATCH CORD CAT. 5E 7 FT. BLANCO	48	2.75	132.00	INMEDIATO
10	LEV 5320-W	UND	TOMACORRIENTE DOBLE POLARIZADO COMERCIAL BLANCO	20	0.65	13.00	INMEDIATO
11	LEV 88003	UND	PLACA DUPLEX COMERCIAL BLANCA	20	0.36	7.20	INMEDIATO
					TOTAL	2,411.26	

CONDIICIONES COMERCIALES:
FORMA DE PAGO: A CONVENIR
TIEMPO DE ENTREGA: INMEDIATO UNA VEZ CONFIRMADO STOCK
VALIDEZ DE LA OFERTA: 8 DÍAS
- Estos precios no incluyen I.V.A.

Atentamente,

Tatiana Mosquera
VENTAS & INGENIERIA DE PROYECTOS
Juan González N35-76 y Juan Pablo Sáinz
PBX: 2 225 1102 / 2155 Ext: 124
tmosquera@martel.com.ec
Movil: 0990435673

Anexo 18: Proforma de servidores

ESPIRAL SISTEMAS

Dirección: Conocoto - Av. Gribaldo Miño y San Pedro de Taboada
Teléfonos 0997642230 - 2099161

PARA: ARQ. LUIS ATAPUMA
INSTITUCIÓN: CENTRO EDUCATIVO "LA PRADERA"
TELÉFONO 2333550

Oferta Económica # 694-ED

SERHPX675421001	**HP DL320e Gen8 E3-1220v2 Hot Plug US Svr** 1U Rack / Intel® Xeon™ Quad-Core E3-1220v2 (3.1GHz, 69W, 8MB) / 4GB (1 x 4GB) UDIMM / No incluye discos duros / HP Ethernet 1Gb 2-port 330i Adapter / HP Smart Array B120i/Zero Memory SATA (0/1/1+0) / 350W Non-hot plug Power Supply / 4 ventiladores Non-hot plug, Non-Redundant / HP iLO Management Engine / 1 año en piezas, mano de obra on site	**MÍNIMO**: 1 servidor + 2 Opciones (Discos, Memoria, Tarjeta de Red y Unidad Optica) **MÁXIMO**: 1 servidor + 4 discos duros + 4 memorias + 1 unidad óptica + 2 tarjetas de red	$ 1,002.00
HDDHPX658071B21	HP 500GB 6G SATA 7.2k 3.5in SC MDL HDD	DL320e/ML350e/DL360e/DL380e/DL385p	$ 212.00
		SUBTOTAL	$ 1,214.00
		IVA	$ 145.68
		TOTAL	**$ 1,359.68**

Atentamente

Ing. Henry Vivanco
hrvivanco@3-s.com
0997642230

Anexo 19: Guía de la Entrevista dirigida a padres de familia sobre la propuesta

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

MAESTRÍA EN REDES Y TELECOMUNICACIONES

ENTREVISTA DIRIGIDA A LOS PADRES DE FAMILIA DEL CENTRO EDUCATIVO LA PRADERA

Objetivo: Indagar sobre los objetivos de la Propuesta

Pregunta	Resp. 1	Resp. 2	Resp. 3
¿Cree usted que aplicar estándares ISO 27001 mediante un Plan de seguridad informática ayudaría al Centro Educativo La Pradera a fortalecer la seguridad de los estudiantes?			
¿Le gustaría conocer sobre los Peligros del uso de Internet en los niños, niñas y adolescentes?			
¿Le gustaría conocer sobre las ventajas de usar el Internet como herramienta de apoyo en la formación de sus hijos(as)?			
Le interesaría saber ¿cuáles herramientas se pueden usar para poner seguridades informáticas en casa?			
¿Qué le parece que el Centro Educativo La Pradera, dicte un Taller sobre Seguridad informática para padres de familia con el objetivo de ayudar a mejorar la seguridad integral de sus hijos(as)?			
¿Le gustaría que el personal docente se capacite en el uso de herramientas de Internet para ayudar a mejorar la formación de sus hijos de una manera segura?			

Anexo 20: Encuesta dirigida a Propietarios y Jefaturas referente a la propuesta

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

MAESTRÍA EN REDES Y TELECOMUNICACIONES

ENCUESTA DIRIGIDA A LOS PROPIETARIOS Y JEFATURAS DEL CENTRO EDUCATIVO LA PRADERA

Objetivo: Indagar sobre los objetivos de la Propuesta

Pregunta	Opciones
¿Qué le pareció la propuesta?	○ No tan buena ○ Buena ○ Muy Buena ○ Excelente
¿Cree que la implementación de el Plan de seguridad informática propuesto permitirá disminuir el riesgo para fortalecer la seguridad del CELP	○ Si ○ No ○ Tal vez
Considera que en esta propuesta se está comprometiendo en la seguridad al talento humano de CELP.	○ Si ○ No ○ Tal vez
Considera que Ofertar la prestación de servicio de seguridad aplicando esta propuesta, el CELP ganará calidad y prestigio en Sangolquí?	○ Si ○ No ○ Tal vez

Tabla A.9: Encuesta dirigida a los propietarios y jefaturas del CELP (Elaborado por: Investigador)

Anexo 21: Comparación de marcas de equipos de comunicaciones

Los siguientes gráficos son elaborados por Tolly engineers, y presentados en (Reese, B., 2011)

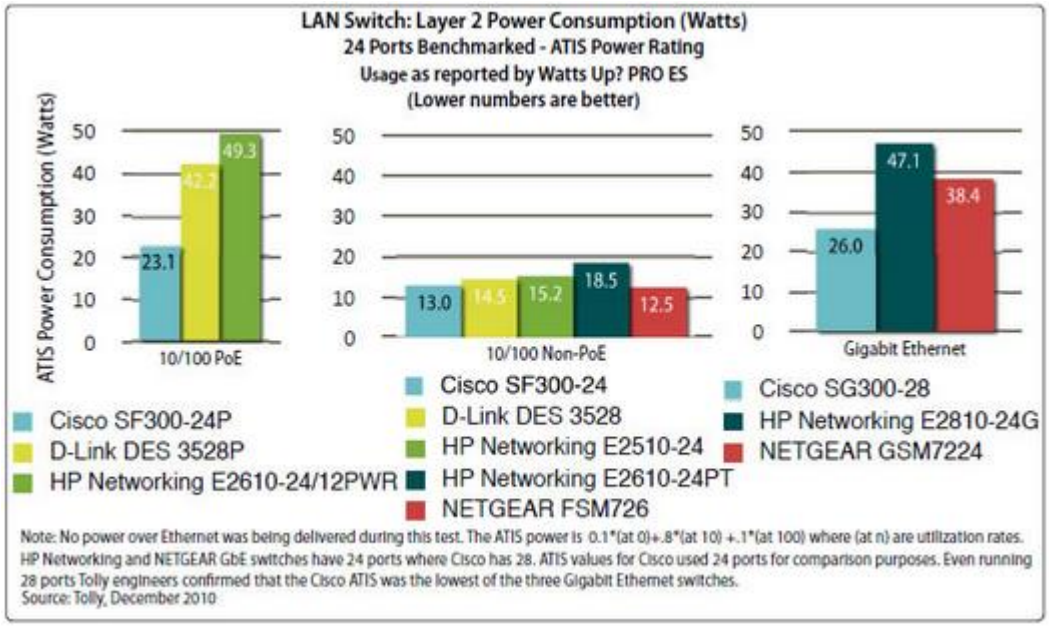


Gráfico: A.13 Comparación de marcas de Switch capa 2, por consumo de energía (Fuente: Reese, B., 2011)

10/100 PoE

System Under Test	Cisco SF300-24P		D-Link DES-3528P		HP Networking E2610-24/12PWR	
Frame size (bytes)	Through put (%)	Latency (µs)	Through put (%)	Latency (µs)	Through put (%)	Latency (µs)
64	100	10.10	99.481	14[1]	100	224.4
128	100	15.2	100	703.4	100	223
256	100	25.7	100	713.6	100	244.2
512	100	46.5	100	733.9	100	250.1
1024	100	87.4	100	774.6	100	300.4
1280	100	107.9	100	795	100	314.6
1518	100	127	100	814.1	100	345.2

Gigabit Ethernet

System Under Test	Cisco SG300-28		HP Networking E2810-24G		NETGEAR GSM7224	
Frame size (bytes)	Through put (%)	Latency (µs)	Through put (%)	Latency (µs)	Through put (%)	Latency (µs)
64	100	3.20	100	4.1	100	4.1
128	100	3.7	100	4.6	100	4.6
256	100	5	100	5.6	100	5.6
512	100	7.4	100	7.6	100	7.7
1024	100	11.5	100	11.7	100	11.7
1280	100	13.5	100	13.7	100	13.8
1518	100	15.4	100	15.6	100	15.7

Note: Throughput results are listed as the percentage of maximum theoretical throughput of 24 10/100 or Gigabit Ethernet ports as appropriate. Uplinks not used for the test. Note: Cisco's GbE switch has 28 ports where HP and NETGEAR's have 24 ports. For purposes of comparison, 24 ports were used on the Cisco switch.
1. Frames were dropped during the 100% load, latency measurement test.

Source: Tolly, December 2010

Gráfico: A.14 Comparación de marcas de Switch capa 2, por rendimiento (Fuente: Reese, B., 2011)

Systems Under Test: 10/100 & Gigabit Ethernet
Non-Stackable, Fully Managed, Non-PoE and PoE LAN Switches

Vendor	Product	Product Class	Software/Hardware Version	CDW Price (USD)
Cisco Systems	Cisco SF300-24 (SRW224-G4-K9-NA)	10/100 Non-PoE	1.0.0.27 21SEP2010 (Same software for all Cisco SUTs)	$215.00
	Cisco SF300-24P (SRW224-G4P-K9-NA)	10/100 PoE		$445.00
	Cisco SG300-28 (SRW2024-K9-NA)	GbE Non-PoE		$499.99
D-Link Systems	D-Link DES-3528 xStack (P1UQ3A8003662)	10/100 Non-PoE	2.60.017 (Same software for both D-Link SUTs)	$508.43
	D-Link DES-3528P xStack (P4LX199000012)	10/100 PoE		$1,174.99 (CompSource)
HP Networking	HP Networking E2610-24PT (J9085A)	10/100 Non-PoE	11.54 (Same software for both HP 2610 SUTs)	$528.99
	HP Networking E2610-24/12PWR (J9086A)	10/100 PoE		$794.42
	HP Networking E2510-24 (J9019B)	10/100 Non-PoE	Q11.26	$342.57
	HP Networking E2810-24G (J9021A)	GbE Non-PoE	N11.25	$1,432.92
NETGEAR	NETGEAR ProSafe FSM726	10/100 Non-PoE	8.0.1.9	$309.00
	NETGEAR ProSafe GSM7224	GbE Non-PoE	8.0.1.4	$716.99

Note:. Systems have at least 24 copper ports with some systems having 2+ uplink/stacking ports. Prices as listed as selling price on CDW website on Jan. 17, 2011 except for the the D-Link DES-3528P which was not listed on CDW, so the price on the CompSource website was used. HP recommended using the E2610-24/24PWR (J9087A), with PoE on 24 ports, but it was not available in the test window.

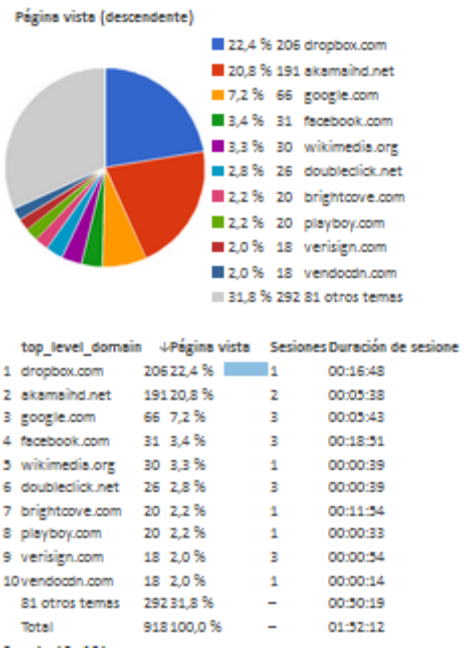
Source: Tolly, January 2011

Gráfico: A.15 Comparación de marcas de equipos de comunicaciones, por precio (Fuente: Reese, B., 2011)

Anexo 22: Reporte generado de sawmill Ver 8.0

Navegación Docentes

Host Summary05/Nov/2013, 1 día

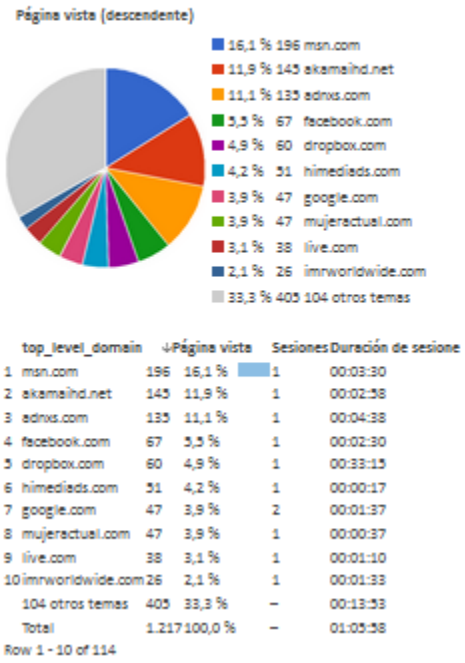


	top_level_domain	↓Página vista		Sesiones	Duración de sesione
1	dropbox.com	206	22,4 %	1	00:16:48
2	akamaihd.net	191	20,8 %	2	00:05:38
3	google.com	66	7,2 %	3	00:05:43
4	facebook.com	31	3,4 %	3	00:18:51
5	wikimedia.org	30	3,3 %	1	00:00:39
6	doubleclick.net	26	2,8 %	3	00:00:39
7	brightcove.com	20	2,2 %	1	00:11:54
8	playboy.com	20	2,2 %	1	00:00:33
9	verisign.com	18	2,0 %	3	00:00:54
10	vendocdn.com	18	2,0 %	1	00:00:14
	81 otros temas	292	31,8 %	–	00:50:19
	Total	918	100,0 %	–	01:52:12

Gráfico: A.16 Host Summary generado del software Sawmill 8.0 (Elaborado por: Investigador)

Navegación estudiantes 5to,6to,7mo

Host Summary05/Nov/2013, 1 día



	top_level_domain	↓Página vista		Sesiones	Duración de sesione
1	msn.com	196	16,1 %	1	00:03:30
2	akamaihd.net	145	11,9 %	1	00:02:58
3	adnxs.com	135	11,1 %	1	00:04:38
4	facebook.com	67	5,5 %	1	00:02:30
5	dropbox.com	60	4,9 %	1	00:33:15
6	himediads.com	51	4,2 %	1	00:00:17
7	google.com	47	3,9 %	2	00:01:37
8	mujeractual.com	47	3,9 %	1	00:00:37
9	live.com	38	3,1 %	1	00:01:10
10	imrworldwide.com	26	2,1 %	1	00:01:33
	104 otros temas	405	33,3 %	–	00:13:53
	Total	1.217	100,0 %	–	01:05:58

Row 1 - 10 of 114

Gráfico: A.17 Host Summary generado del software Sawmill 8.0 (Elaborado por: Investigador)

Anexo 23: Documento de aprobación para realizar la investigación en el CELP