UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS

Tema:

"Políticas de Seguridad de la información basado en la Norma ISO/ICE 27002:2013 para la Dirección de Tecnologías de Información y Comunicación de la Universidad Técnica de Ambato"

Proyecto de Trabajo de Graduación. Modalidad: Proyecto de Investigación, presentado previo la obtención del título de Ingeniero en Sistemas Computacionales e Informáticos.

SUBLÍNEA DE INVESTIGACIÓN: Seguridad de unidades informáticas

AUTOR: Torres Núñez Elizabeth Magdalena

PROFESOR REVISOR: Ing. Galo Mauricio López Sevilla

Ambato – Ecuador

Julio – 2015

APROBACIÓN DEL TUTOR

En mi calidad de tutor del Trabajo de Investigación sobre el tema: "**Políticas de Seguridad de la información basado en la Norma ISO/ICE 27002:2013 para la Dirección de Tecnologías de Información y Comunicación de la Universidad Técnica de Ambato**.", de la señorita Torres Nuñez Elizabeth Magdalena, estudiante de la Carrera de Ingeniería en Sistemas Computacionales e Informáticos, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, considero que el informe investigativo reúne los requisitos suficientes para que continúe con los trámites y consiguiente aprobación de conformidad con el numeral 7.2 de los Lineamientos Generales para la aplicación de Instructivos de las Modalidades de Titulación de las Facultades de la Universidad Técnica de Ambato.

Ambato julio, 2015

EL TUTOR

Ing. Galo Mauricio López

AUTORÍA

El presente Proyecto de Investigación titulado: "**Políticas de Seguridad de la información basado en la Norma ISO/ICE 27002:2013 para la Dirección de Tecnologías de Información y Comunicación de la Universidad Técnica de Ambato**", es absolutamente original, auténtico y personal, en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato julio, 2015

EL AUTOR

_____

Elizabeth Magdalena Torres Núñez

CC: 180466647-5

DERECHOS DE AUTOR

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

Cedo los derechos de mi Trabajo de Titulación, con fines de difusión pública, además autorizo su reproducción dentro de las regulaciones de la Universidad.

Ambato julio, 2015

Elizabeth Magdalena Torres Núñez

CC: 180466647-5

APROBACIÓN DE LA COMISIÓN CALIFICADORA

La Comisión Calificadora del presente trabajo conformada por los señores docentes Ing. Dennis Chicaiza e Ing. Jaime Ruiz, revisarón y aprobarón el Informe Final del trabajo de Investigaciòn titulado **"Políticas de Seguridad de la información basado en la Norma ISO/ICE 27002:2013 para la Dirección de Tecnologías de Información y Comunicación de la Universidad Técnica de Ambato"**, presentado por la Srta. Elizabeth Magdalenan Torres Nuñez de acuerdo al numeral 9.1 de los Lineamientos Generales para la aplicación de Instructivos de las Modalidades de Titulación de las Facultades de la Universidad Técnica de Ambato.

Ambato julio, 2015

_____

Ing. Mg. Vicente Morales
PRESIDENTE DEL TRIBUNAL

_____ _____

Ing. Dennis Chicaiza
DOCENTE CALIFICADOR

Ing. Jaime Ruiz
DOCENTE CALIFICADOR

DEDICATORIA

El presente trabajo se lo dedico a Dios por darme la oportunidad de estar en este mundo maravilloso y porque día a día me da fuerzas para seguir adelante, por regalarme una familia maravillosa.

También se la dedico a mis padres, quienes han estado conmigo en todo momento, brindándome su apoyo y comprensión, a mis hermanos por su apoyo.

A mis abuelitos Ángela y Ernesto que siempre están pendientes dándome ánimos para salir adelante cuidando de mi bienestar, y se las dedico a mis abuelitos Transito y Francisco que aunque no están físicamente siempre me estarán cuidando desde el cielo.

A toda mi familia, amigos y amigas que de forma directa o indirecta han colaborado con la realización de este trabajo.

Elizabeth Magdalena Torres

AGRADECIMIENTO

Agradezco a Dios por bendecirme a cada instante y poder abrir mis ojos cada día y permitirme culminar con este trabajo.

A mis padres porque desde pequeña me inculcaron valores los que me han servido para llegar a alcanzar esta meta, por brindarme su apoyo en todo momento, por ayudarme a cumplir con mi sueños y por el simple hecho de darme la vida.

A la Facultad de Ingeniería en Sistemas, Electrónica e Industrial por infundir los conocimientos para iniciar una vida profesional, a los docentes que me brindaron sus conocimientos.

A mi tutor el Ing. Galo López por guiarme en el desarrollo de este proyecto.

Mi más sincero agradecimiento a todos quienes fueron participes de la culminación de este trabajo.

Elizabeth Magdalena Torres

PÁGINAS PRELIMINARES

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN EJECUTIVO

La Dirección de Tecnología de Información y Comunicación DITIC de la Universidad Técnica de Ambato UTA, es la encargada de implementar y mantener toda la infraestructura tecnológica y activos de información de la universidad.

Con el fin de que todos los activos de información se encuentren protegidos se propone políticas de seguridad de la información basados en la norma ISO 27002 versión 2013, las mismas que permitirán proteger la información de accesos no autorizados, daños físicos o ambientales, y de plagios.

Para el desarrollo del presente proyecto como primer paso se realizó un análisis de la situación actual de la DITIC, mediante una entrevista realizada al director, y un análisis a la red inalámbrica de la universidad, lo que ayudo a tener una visión de la protección que se le da a la información.

Luego del análisis, el próximo paso fue el desarrollo de las políticas de seguridad basándonos en la norma Internacional ISO 27002 en su versión 2013, esta norma no es certificable es un manual de buenas prácticas, en la que el principal objetivo es proteger la información, la misma que es un eje primordial en cualquier organización.

Se desarrollaron políticas como control de acceso, perímetros de seguridad, proceso de contratación y cesación de actividades de empleados entre las más importantes. Luego de realizar las políticas de seguridad los dos últimos dominios tratan específicamente sobre la continuidad del negocio y cumplimiento de las políticas de seguridad creadas en los dominios anteriores.

SUMMARY

The Department of Information and Communication Technology DICT of the Technical University of Ambato UTA is in charge of implementing and maintaining all the technological infrastructure and information assets of the university.

In order for all the information assets to be protected, information security policies based on ISO 27002 version 2013 are proposed, making it possible to protect the information and prevent unauthorized access, physical and environmental damage, and plagiarism.

The first step to develop this project was to perform the analysis of the current situation of the DICT through interviews to the people in charge of administration. This helped to have a vision of the protection that is given to information.

After the analysis, the next step was to develop security policies based on the international standard ISO27002-2013. This standard is not certifiable but it is a manual of good practices whose main objective is information, which is a core idea in any organization.

Policies were developed such as access control, security perimeters, the hiring of employees and termination processes, among the most important. After developing the security policies, the last two domains specifically address business continuity and fulfilling security policies created in the past domains.

INTRODUCCIÓN

El presente trabajo de investigación "**Políticas de Seguridad de la información basado en la Norma ISO/ICE 27002:2013 para la Dirección de Tecnologías de Información y Comunicación de la Universidad Técnica de Ambato.**", consta de cinco capítulos los mismos que se detallan a continuación:

El primer capítulo está compuesto por planteamiento del problema, la delimitación, justificación y objetivos del tema de investigación para iniciar con el análisis de las necesidades de la DITIC y de los empleados quienes son beneficiarios de la seguridad en la información.

El segundo capítulo contiene los antecedentes investigativos tales como tesis, documentos, revistas, que contienen temas similares al problema identificado en la DITIC; también contiene el marco teórico en el cual consta la fundamentación bibliográfica, papers, internet fuentes que ayudaron a fundamentar el tema de investigación y finalmente contiene la propuesta de solución que el investigador propone.

El tercer capítulo comprende la modalidad de la investigación aplicada en el desarrollo del presente proyecto, la técnica de investigación utilizada para obtener la información necesaria para el desarrollo del proyecto mediante entrevista al director de la DITIC, así como también la definición de las actividades para el desarrollo de la propuesta.

El cuarto capítulo comprende el desarrollo de la propuesta, una descripción de los objetivos y servicios que brinda, así como también, el análisis de la situación actual de la DITIC mediante una entrevista realizada al director. Comprende también un análisis a la red de la facultad de ingeniería en sistemas computacionales e informáticos FISEI para determinar las

necesidades que ayuden a establecer las políticas de seguridad de la información, y el desarrollo de políticas de seguridad de la información basada en la norma internacional ISO 27002 versión 2013.

Finalmente, en el quinto capítulo se encuentran las conclusiones y recomendaciones obtenidas del trabajo de investigación realizado.

CAPÍTULO I

1. EL PROBLEMA

1.1.Tema

‘‘Políticas de Seguridad de la información basado en la Norma ISO/ICE 27002:2013 para la Dirección de Tecnologías de Información y Comunicación de la Universidad Técnica de Ambato’’.

1.2.Planteamiento del problema

1.2.1. Contextualización

A nivel mundial la mayoría de las empresas dedicadas o no a tecnologías de información brindan servicios y procesos en red. Desde los inicios de las computadoras, la seguridad de la información ha sido de vital importancia, en la actualidad se brinda mayor importancia a contar con buenos mecanismos de seguridad de la información debido a las diversas vulnerabilidades que la red tiene. Existen estándares internacionales que proporcionan mecanismos de seguridad estudiados y puestos a prueba con excelentes resultados. Al seguir una recomendación de un estándar internacional concerniente a seguridad de la información es tener un protocolo en común para la medida y gestión de los riesgos informáticos.

En Ecuador, varias instituciones públicas y privadas contextualizan a la información como un problema tecnológico, sin tener en cuenta que la seguridad de la información es un problema organizativo y de gestión, provocando que las instituciones afronten ataques provenientes de todos los ángulos. Contar con tecnología sofisticada no es suficiente;

gestionar significa conocer la situación actual y saber a dónde se quiere llegar, es decir, determinar un objetivo y tomar las acciones necesarias para lograrlo. La seguridad de la información involucra a toda la institución, por lo tanto, se debe fomentar un cambio cultural en los usuarios, para concienciar acerca de importancia de la seguridad.

Las universidades cuentan con información esencial para el mejoramiento académico, pero esta información debe contar con las tres características principales para definir que su información sea segura; estas características son: integridad, confidencialidad y disponibilidad.

Algunas de las universidades ya cuentan con normas de seguridad de la información como por ejemplo la universidad Politécnica Salesiana Sede Guayaquil, quien tiene implementada la norma ISO 27002 versión 2005.

La UTA no cuenta con ningún estándar internacional implementado con respecto a seguridad de la información, que ayude a proteger y resguardarla. Esto provoca que personas externas tengan acceso a información importante para la universidad, con la utilización de las nuevas tecnologías de información que pueden llegar a vulnerar información no protegida.

1.3.Delimitación

Área académica: Administrativas Informáticas.
Línea de Investigación: Normas y Estándares.
Sublínea de Investigación: Seguridad de Unidades Informáticas.
Delimitación espacial: Dirección de Tecnología de Información y Comunicación de la Universidad Técnica de Ambato DITIC**.**
Delimitación temporal: La duración del proyecto es de 6 meses a partir de la fecha de aprobación del perfil, por parte del Honorable Consejo Directivo de la Facultad.

1.4.Justificación

La información es un recurso de vital importancia en la UTA, por esta razón debe existir técnicas, procedimientos y actividades que la aseguren, además de la seguridad física que se establece en los equipos que se almacena la información, es vital la seguridad lógica, que radica en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo permita acceder a la información a personal autorizadas para su manipulación o gestión. La universidad no cuenta con una metodología de gestión de seguridad clara y estructurada para reducir el riesgo de pérdida, corrupción o robo de la información.

Las políticas de seguridad basado en la norma ISO/ICE 27002:2013 consiste en establecer un conjunto de políticas y procedimientos que normalizan la gestión de la información, proporciona una visión más amplia de los problemas de seguridad relacionados con la información y recurso humano encargado de gestionarla. Esto permite tener una metodología de gestión de la información clara y segura, además, es un estándar internacional que en su versión 2013 cuenta con nuevos dominios y controles que buscan mitigar el impacto o la posibilidad de ocurrencia de los diferentes riesgos a los cuales se encuentra expuesta la organización.

Los beneficios que alcanzará la universidad con este proyecto serán integridad, confidencialidad y disponibilidad de la información, además de resguardarla ante las diferentes vulnerabilidades y acceso no autorizado de personas externas a la universidad.

Por lo expuesto anteriormente y gracias al apoyo de la DITIC de la universidad se justifica el desarrollo del presente proyecto, el mismo que de ser aplicado brindará un gran aporte a la comunidad universitaria.

1.5.Objetivos

1.5.1. Objetivo general

Elaborar políticas de seguridad de la información en base a parámetros de la norma ISO/IEC 27002:2013 en la Dirección de Tecnologías de Información y Comunicación de la Universidad Técnica de Ambato.

1.5.2. Objetivos específicos

- Analizar la protección de la información actual contra acceso no autorizado.
- Establecer lineamientos de seguridad de la información mediante parámetros de la norma ISO/IEC 27002:2013.
- Elaborar un plan de evaluación continua de seguridad de la información mediante responsabilidades y procedimientos.

CAPÍTULO II

2. MARCO TEÓRICO

2.1. Antecedentes Investigativos

Tania Verónica Guachi Aucapiña, en su proyecto de investigación realizado en la Cooperativa de Ahorro y Crédito San Francisco LTDA, creado en la Universidad Técnica de Ambato en su conclusión afirma que:
"El contenido de la ISO 27001 está orientado al tratamiento de seguridad de la información mediante la gestión de riesgos, ya que describe la manera de mantener y mejorar la seguridad de los activos de información de cualquier organización."[1].

Daniel Romo Villafuerte y Joffre Valarezo Constante, autores del proyecto de investigación de la norma ISO 27002 para el departamento de sistemas de la Universidad Politécnica Salesiana sede Guayaquil, creado en la Universidad Politécnica Salesiana sede Guayaquil. En una de sus conclusiones afirma que:
"Es importante recalcar que si se cumple al 100% con las políticas desarrolladas para la Universidad Politécnica Salesiana sede Guayaquil, no se garantiza que no tenga problemas de seguridad ya que no existe la seguridad al 100%; con el manual de políticas de seguridad de la información y con el cumplimento de las mismas da lugar a minimizar los riesgos asociados a los activos reduciendo impactos, fuga de información y perdidas económicas originados por la carencia de las normas y políticas de seguridad de la información."[2].

Por otra parte los Ingenieros Mauricio Javier Baldeón Garzón y Christian Alfredo Coronel Guerrero, en su proyecto de investigación Plan maestro de Seguridad de la información para

la UTIC de la ESPE con lineamientos de la norma ISO/IEC 27002, creado en la Escuela Politécnica del Ejército. En una de sus recomendaciones afirma que:
"Se realice un análisis integral de los riesgos físicos (eléctricos, fuego, inundaciones, entre otros) a fin de elaborar un plan de mejoras en la seguridad física del edificio donde se encuentra ubicado el Data Center institucional."[3].

2.2.Fundamentación Teórica

Seguridad Informática

"La seguridad de la información es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable."[4].

Tipos de Seguridad

Activa

"Comprende el conjunto de defensas o medidas cuyo objetivo es evitar o reducir los riesgos que amenazan al sistema."[5].

"Ejemplos: impedir el acceso a la información a usuarios no autorizados mediante introducción de nombres de usuario y contraseñas; evitar la entrada de virus instalando un antivirus; impedir, mediante encriptación, la lectura no autorizada de mensajes."[5].

Pasiva

"Está formada por las medidas que se implementan para, una vez producido el incidente de seguridad, minimizar su repercusión y facilitar la recuperación del sistema; por ejemplo, teniendo siempre al día copias de seguridad de los datos."[5].

ISO/IEC 27000

"Es un conjunto de estándares desarrollados –o en fase de desarrollo- por ISO (*International Organization for Standardization*) e IEC (*International Electrotechnical Commision*), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización (pública, privada, grande o pequeña)." [6].

"A semejanza de otras normas ISO, la 27000 es realmente una serie de estándares, donde las normas principales son la ISO/IEC 270001 y la ISO/IEC 270002."[6].

ISO 27002

"La norma ISO 27002 fue publicada originalmente como un cambio de nombre de la norma 17799 ISO existente, un código de prácticas para la seguridad de la información. Básicamente describe cientos de potenciales controles y mecanismos de control, que pueden ser implementadas, en teoría, con sujeción a las directrices proporcionadas en la norma ISO 27001." [7].

"Los lineamientos y principios generales para iniciar, implementar, mantener y mejorar la gestión de seguridad de la información dentro de una organización estándar. Los controles reales que figuran en la norma tienen por objeto atender las necesidades específicas identificadas por medio de una evaluación de riesgos formal. La norma también tiene por objeto proporcionar una guía para el desarrollo de normas de seguridad de la organización y las prácticas eficaces de gestión de la seguridad y para ayudar a construir la confianza en las actividades interinstitucionales."[7].

HISTORIA ISO/IEC 27002

"Los requisitos codificados en ISO 27001 se expanden y se explica en la norma ISO 27002 en la forma de una guía. El manual fue publicado por primera vez en el año 2000 en ese

tiempo con la designación de "17799 ISO", bajo el título “Tecnología de la información - Técnicas de Seguridad- Código de prácticas para la gestión de seguridad de la información”. En el año 2007 este fue revisado y alineado a la familia de estándares 27 K y la designación fue cambiada a la norma ISO 27002.”[8].

“Con el desarrollo de la norma ISO 27002, se ofrecieron las prácticas comunes (a menudo, también conocidas como las mejores prácticas) como los procedimientos y métodos de probada eficacia en la práctica, lo que podría adaptarse a las necesidades específicas dentro de las empresas.”[8].

“Con el fin de explicar la importancia de seguridad de la información para las empresas, los riesgos para la seguridad de la información de una empresa y la necesidad de haber dirigido y acordado medidas ("controles") en el marco de un SGSI(Sistema de Gestión de Seguridad de la Información) se establecen. Pasos necesarios para la identificación y evaluación de riesgos de seguridad se describen en el fin de determinar la necesidad de proteger la información y los sistemas de información.”[8].

La norma ISO 27002 no es certificable pero es el primer anexo que se debe cumplir para obtener la certificación de la norma ISO 27001, los controles de esta norma ayudan y son reutilizables para el cumplimiento de la norma mencionada de acuerdo al siguiente gráfico:

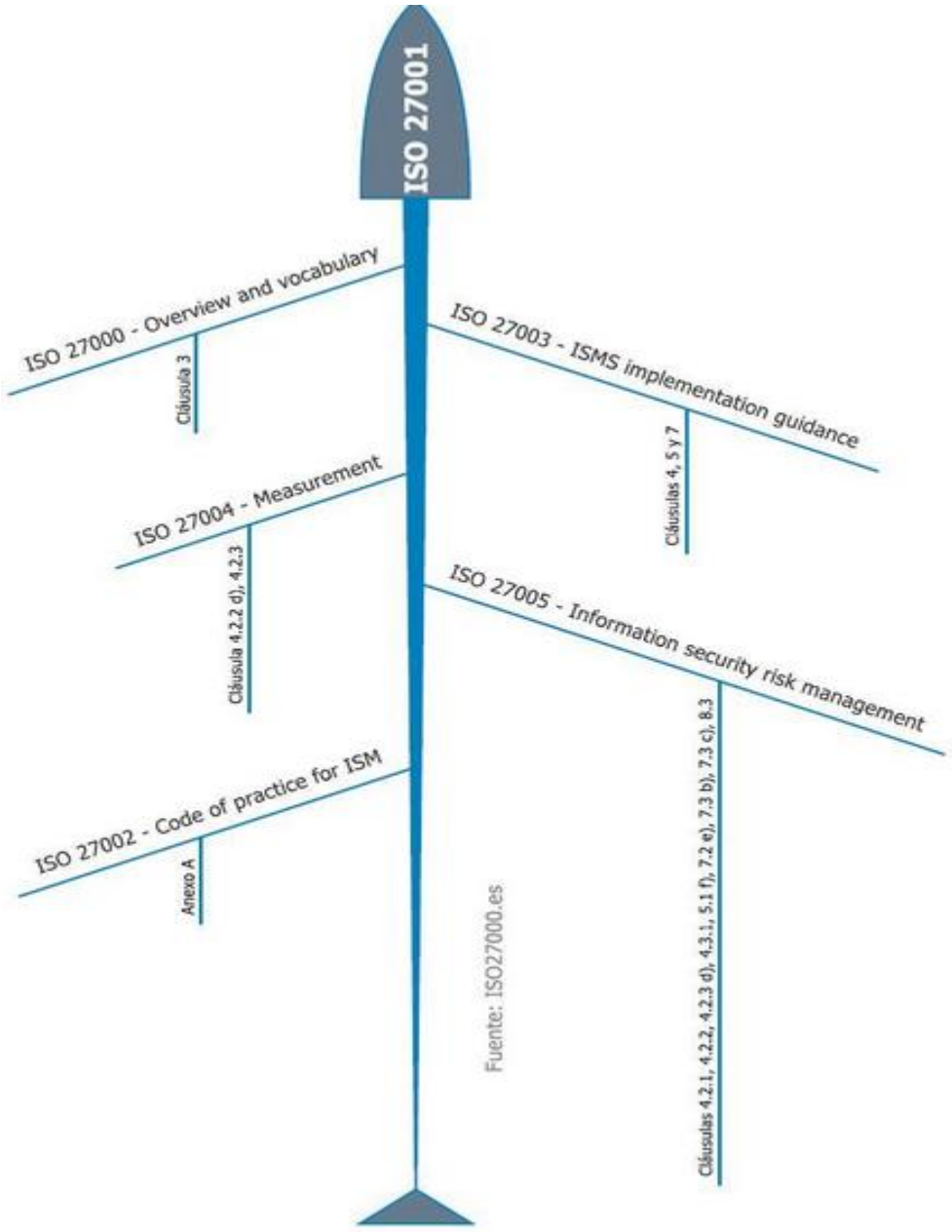


Gráfico Nº 1: Requerimientos para certificación ISO 27001

Elaborado por: ISO27000.es

Fuente: [10].

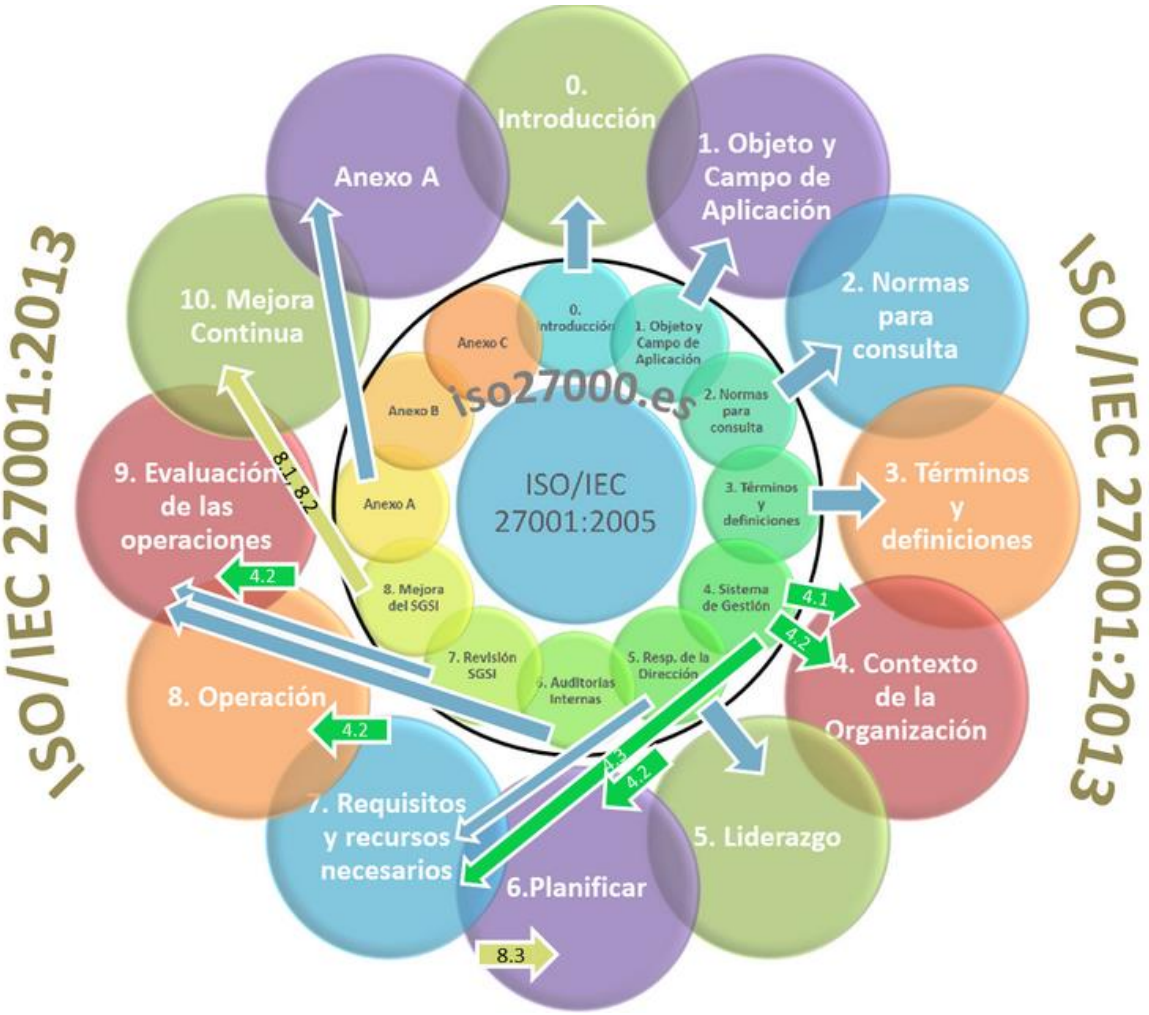


Gráfico Nº 2: ISO 27001 – ISO 27002

Elaborado por: ISO27000.es

Fuente: [10].

"La norma ISO 27000 en su versión 2013 cuenta con 19 secciones, 35 objetivos de control y 114 controles específicos. Cabe recalcar que las 5 secciones iniciales, son generales para la familia de las normas 27000, es por esta razón que consta de 14 secciones o dominios, las 5 secciones iniciales son:

DOMINOS Y OBJETIVOS DE CONTROL DE LA NORMA ISO/IEC 270002:2013

1. Políticas de seguridad.
   1.1. Directrices de la dirección en seguridad de la información.
2. Aspectos organizativos de la seguridad de la información.
   2.1. Organización interna.
   2.2. Dispositivos para movilidad y teletrabajo.
3. Seguridad ligada a los recursos humanos.
   3.1. Antes de la contratación.
   3.2. Durante la contratación.
   3.3. Cese o cambio de puesto de trabajo.
4. Gestión de activos.
   4.1. Responsabilidad sobre los activos.
   4.2. Clasificación de la información.
   4.3. Manejo de los soportes de almacenamiento.
5. Control de acceso.
   5.1. Requisitos de negocio para el control de acceso.
   5.2. Gestión de acceso de usuario.
   5.3. Responsabilidad del usuario.
   5.4. Control de acceso a sistemas y aplicaciones.
6. Cifrado.
   6.1. Controles criptográficos.
7. La seguridad física y ambiental.
   7.1. Áreas seguras.
   7.2. Seguridad de los equipos.
8. Seguridad en la operativa.
   8.1. Responsabilidades y procedimientos de operación.
   8.2. Protección contra código malicioso.
   8.3. Copia de seguridad.
   8.4. Registro de actividad y supervisión.

8.5. Control del software en explotación.

8.6. Gestión de vulnerabilidades técnicas.

8.7. Consideraciones de auditorías de los sistemas de información.

9. Seguridad en las telecomunicaciones.

9.1. Gestión de la seguridad en las redes.

9.2. Intercambio de información con partes externas.

10. Adquisición, desarrollo y mantenimiento de los sistemas de información.

10.1. Requisitos de seguridad de los sistemas de información.

10.2. Seguridad de los procesos de desarrollo y soporte.

10.3. Datos de prueba.

11. Relaciones con suministradores.

11.1. Seguridad de la información en las relaciones con suministradores.

11.2. Gestión de la prestación de servicios por suministradores.

12. Gestión de los incidentes en la seguridad de la información.

12.1. Gestión de incidentes de seguridad de la información y mejoras.

13. Aspectos de seguridad de la información en la gestión de la continuidad del negocio.

13.1. Continuidad de seguridad de la información.

13.2. Redundancias.

14. Cumplimiento.

14.1. Cumplimiento de los requisitos legales y contractuales.

14.2. Revisiones de la seguridad de la información.” [9].

Control

Son “las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. También puede ser utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.” [10].

Control correctivo

"Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas relevantes. Supone que la amenaza ya se ha materializado pero que se corrige." [10].

Control detectivo

"Control que detecta la aparición de un riesgo, error, omisión o acto deliberado. Supone que la amenaza ya se ha materializado, pero por sí mismo no la corrige." [10].

Control disuasorio

"Control que reduce la posibilidad de materialización de una amenaza. Por ejemplo, por medio de avisos o de medidas que llevan al atacante a desistir de su intención." [10].

Control preventivo

"Control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse." [10].

Gestión de activos de la información

"Desde esta perspectiva la gestión de la información surge como un nuevo concepto dentro del campo de la ciencia de la información, orientado al manejo de la inteligencia corporativa de una organización, que permite la estructuración interna a las organizaciones y les permite reaccionar ante los cambios de su entorno apoyándose en el uso de la información y de los recursos de información disponibles.

Esta situación lleva a las concepciones más recientes defendidas por la Gestión de la Información (GI), en el sentido de que las organizaciones deben ser consideradas fundamentalmente como sistemas de información.

Algunos autores coinciden en que la GI, plantea que "gerencia es todo lo que se refiere a la obtención de la información adecuada, para la persona adecuada, a su precio adecuado, en el tiempo y lugar adecuado, para tomar la decisión adecuada."

Su objetivo es el de incrementar los niveles de eficiencia y efectividad dentro de una organización. Este proceso se produce a través de la integración adecuada de los recursos

humanos, las políticas, las actividades y procedimientos, el hardware, el software y los datos" [11].

Criptografía

"El termino criptografía proviene de dos vocablos griegos κρύπτω, que significa "escondido", y γράφως, "escritura". Más tarde se añade el sufijo –ía para conferirle el carácter de conocimiento o tratado. Según esta definición de carácter etimológico, la criptografía es la ciencia que estudia la escritura oculta" [12].

Pero aún no se puede precisar más este concepto, y así, esta disciplina, es entendida como el arte de escribir en un lenguaje convenido mediante el uso de claves o cifras, es decir, la criptografía enseña a diseñar cifrarios (expresión sinónima de código secreto o escritura secreta); la operación inversa es "criptoanálisis": interpretar mediante análisis los cifrarios construidos por los criptógrafos" [12].

Confidencialidad

"La confidencialidad de la información define en ámbito en el que dicha información puede ser conocida dentro de la organización, identificando personas o perfiles que pueden tener acceso a ella" [13].

Integridad

"La integridad de la información define el grado de exactitud con que dicha información responde realmente lo que dice representar" [13].

"La definición de integridad debe comprender los términos de exacta, autorizada y completa" [13].

Disponibilidad

"La disponibilidad de la información representa para los usuarios la garantía de disponibilidad de utilización cuando sea requerida o necesitada" [13].

2.3.Propuesta de solución

Con la elaboración de políticas de seguridad de la información basado en la norma ISO/ICE 27002:2013 para la DITIC de la UTA se busca dar seguridades y disminuir la vulnerabilidad de acceso a la información y establecer el camino para que la universidad promueva la búsqueda de la certificación ISO/IEC 27001.

CAPÍTULO III

3. METODOLOGÍA

3.1.Modalidad de la investigación

La presente investigación considerará las siguientes modalidades:
De campo.- Se realizó una investigación de campo, así como también, se aplicó una entrevista y observación en la DITIC.
Bibliográfica documentada.- Se sustentó en revistas, libros, periódicos, internet, tesis, como fuentes para recolectar información, que sirvió para la realización de este proyecto de investigación.

3.2.Población y muestra

La presente investigación por su tipo, no amerita población.

3.3.Recolección de información

Para la recolección de la información se aplicó una entrevista a la persona encargada de la administración de la DITIC de la UTA. Además de la observación que se realizó. Se recolectó información a través de libros físicos y digitales, artículos científicos, internet, guía de entrevista, guía de observación.

3.4.Procesamiento y análisis de información

Para el procesamiento y análisis de la información se aplicó los siguientes procedimientos:

- Elaboración y validación del instrumento de recolección de datos.
- Organización de la información.
- Tabulación de la información recolectada.
- Informe de resultados.

3.5. Desarrollo del proyecto

Para el desarrollo de proyecto se realizó las siguientes actividades:

- Análisis de la protección de la información actual contra acceso no autorizado
  - Análisis de la situación actual
  - Análisis FODA de la norma ISO 27002
  - La empresa
  - Estructura organizacional
  - Análisis de las encuestas
  - Análisis de vulnerabilidades

- Establecimiento de lineamientos de seguridad de la información mediante parámetros de la norma ISO/IEC 27002:2013
  - Aspectos organizativos de la seguridad de la información.
  - Seguridad ligada a los recursos humanos.
  - Gestión de activos Control de acceso.
  - Cifrado.
  - La seguridad física y ambiental.
  - Seguridad en la operativa.
  - Seguridad en las telecomunicaciones.
  - Adquisición, desarrollo y mantenimiento de los sistemas de información.

- Relaciones con suministradores.
- Gestión de los incidentes en la seguridad de la información.

- Elaboración de un plan de evaluación continua de seguridad de la información mediante responsabilidades y procedimientos.
  - Aspectos de seguridad de la información en la gestión de la continuidad del negocio.
  - Cumplimiento.

CAPÍTULO IV

4. PROPUESTA

4.1.Análisis de la protección de la información actual contra acceso no autorizado

4.1.1. Análisis de la situación actual

Según la entrevista realizada al director de la DITIC de la UTA se pudo constatar que no cuentan con políticas definidas sobre protección de la información, cabe recalcar que se está reestructurando la dirección por tal motivo no se cuenta con un responsable concreto para seguridad, pero se lleva un control de acceso a los diversos sistemas y plataformas que oferta la universidad empíricamente.

4.1.2. Análisis FODA de la norma ISO 27002

	Fortalezas	Debilidades
Análisis Interno	▪ Es una norma internacional adoptada por varias organizaciones. ▪ Es una norma de adaptación fácil. ▪ Es una guía para mejorar las prácticas de la seguridad de la información.	▪ Falta de profesionales especializados en normas internacionales. ▪ Desconocimiento de la existencia de la Norma ISO, para seguridad de la información.
	Oportunidades	**Amenazas**
Análisis Externo	▪ Se puede aplicar en cualquier institución por ser una norma internacional. ▪ La organización puede elegir los controles necesarios para la protección de la información.	▪ No existen aplicaciones específicas para la implementación. ▪ La norma no es certificable.

Tabla Nº1.- Análisis FODA

Elaborado por: Elizabeth Torres

4.1.3. La empresa

"La Dirección de Tecnología de Información y Comunicación de la Universidad Técnica de Ambato cumple con un objetivo que es:

- Brindar la administración, control, desarrollo, mantenimiento del Software, Hardware y necesidades técnicas, logísticas y de capacitación en el área informática para el beneficio de la comunidad universitaria y la colectividad."[14].

"Además cumple con objetivos específicos que son:

- Administrar y controlar las aplicaciones informáticas y redes de comunicación.

- Garantizar la integridad, confidencialidad y disponibilidad de la información.
- Mantener el inventario y existencias actualizado del material informático.
- Desarrollar los Sistemas Informáticos para las diferentes áreas.
- Capacitación dirigida a los funcionarios universitarios en las diferentes áreas universitarias en temas que competen al DITIC."[14].

MISIÓN

"Diseñar, desarrollar e implementar los sistemas de información de modo eficaz y eficiente como apoyo logístico y soporte técnico a las actividades académicas, de gestión y administración para la toma de decisiones, soportado en una infraestructura de sistemas de cómputo y de redes de comunicación, que proporcione servicios especializados que coadyuven a la formación integral de los universitarios en el marco de un modelo educativo."[14].

VISIÓN

"Coordinar y desarrollar con éxito los sistemas de información que apoyan las actividades académicas, así como la gestión y administración de la Universidad Técnica de Ambato. Sistema de información automatizado que procesa toda información institucional generada en las distintas unidades organizacionales y el servicio de redes de comunicación que se presta a través de la red y que permiten el efectivo enlace y comunicación a nivel nacional e internacional entre las diversas Facultades, Departamentos, comunidad de docentes, estudiantes, empleados y trabajadores, enfocado al tangible avance científico–tecnológico, construyendo la universidad de excelencia."[13].

4.1.4. Estructura organizacional

La Dirección de Tecnología de Información y Comunicación de la Universidad Técnica de Ambato cuenta con la siguiente estructura organizacional:

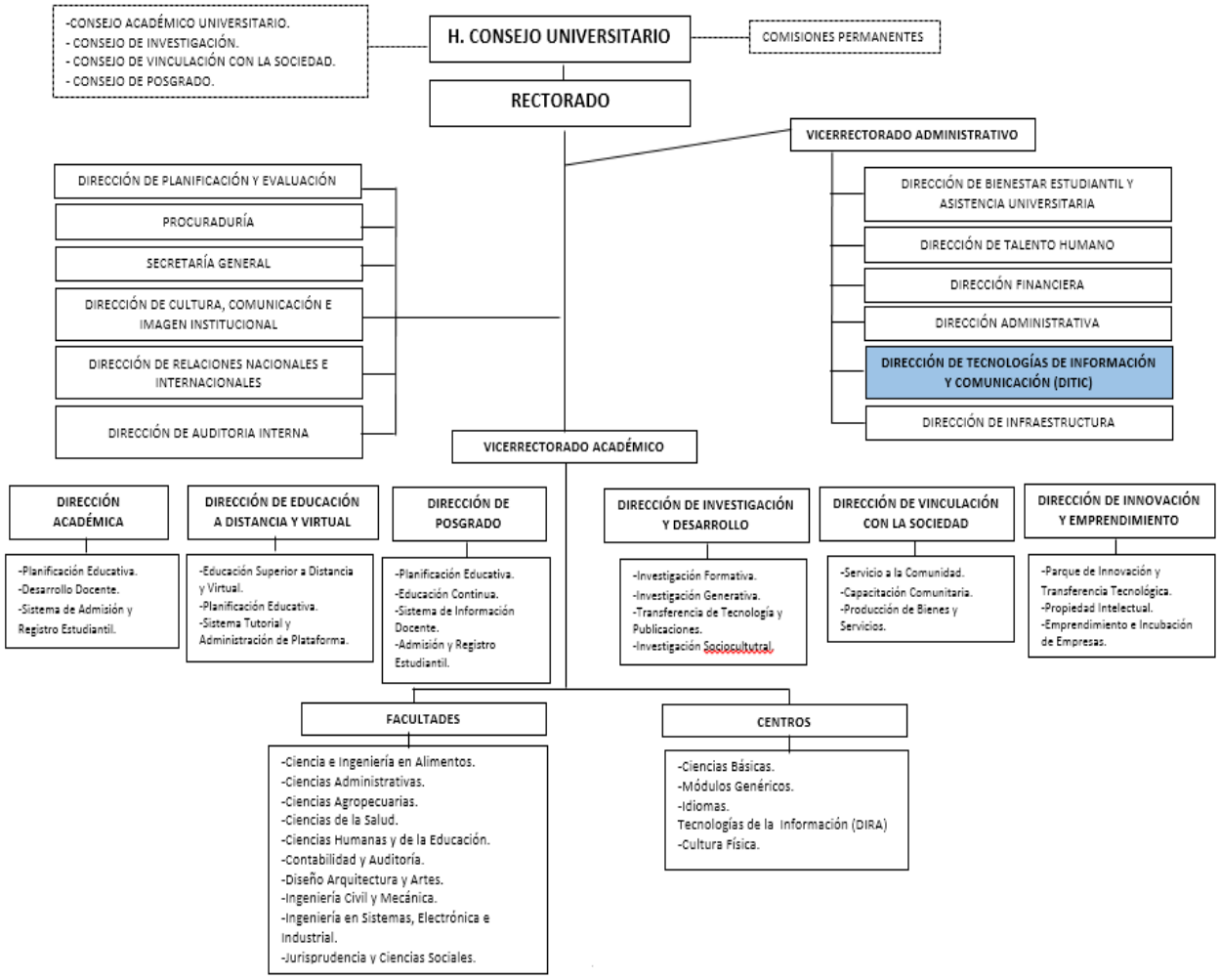


Gráfico Nº 3: Estructura Orgánica de la UTA

Elaborado por: Elizabeth Torres

Fuente: [14].

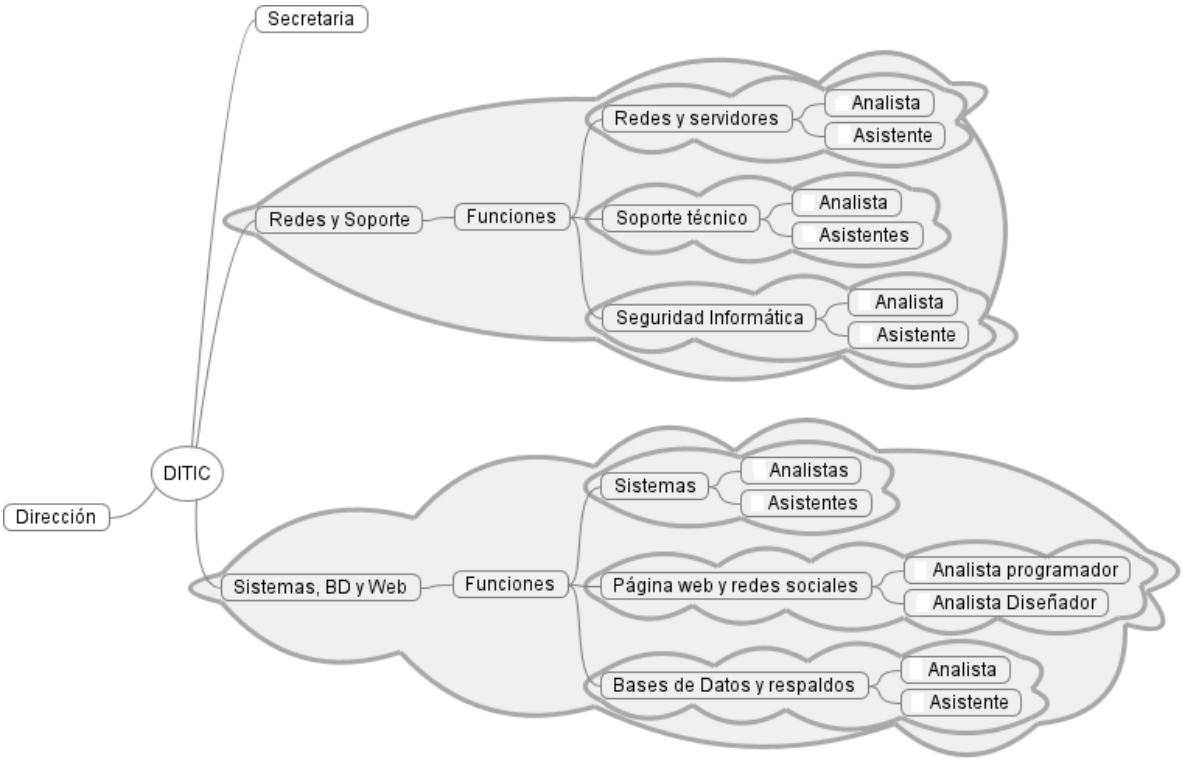


Gráfico Nº 4: Organigrama de Funciones del DITIC a futuro.

Elaborado por: Elizabeth Torres

Fuente: [14].

4.1.5. Análisis de las encuestas

Para el desarrollo del presente proyecto de investigación se realizó la entrevista al Ingeniero Fernando Garcés director de Tecnologías de Información y Comunicación, con la que pudo comprobar que la Universidad Técnica de Ambato no cuenta con políticas de seguridad de la información.

¿Se cuenta con políticas de seguridad de la información?

No se cuenta con políticas establecidas, pero si se controla de diferente manera el ingreso a los diversos sistemas que utiliza la universidad. Como por ejemplo a los estudiantes se les otorga un pin para poder ingresar al Utamático a revisar sus calificaciones. A las secretarias para el sistema de matriculación se les habilita mediante la dirección IP de los computadores.

¿Se cuenta con un área exclusiva para la seguridad de la Información?

Mediante el reglamento interno de la Universidad está aprobada el área de gestión de seguridad de la información, pero no se cuenta con un manual de definición y descripción de funciones y con una persona específica para ocupar ese puesto.

¿Se cuenta con un inventario de activos actualizado? Cada que tiempo se lo actualiza.

La Universidad Técnica de Ambato cuenta con un administrador de bienes quien es el encardado de realizar el inventario de activos, si no existiere la adquisición de algún equipo o enser, el inventario se lo actualiza cada año.

¿Para las áreas seguras se cuenta con control de acceso de personal?

Si se cuenta con control de acceso, por ejemplo para ingresar al cuarto de equipos se cuenta con un biométrico, además se encuentran instaladas cámaras de vigilancia en toda la Universidad.

¿En caso de algún fallo en el cableado de datos o en los diferentes sistemas se encuentran preparados para una pronta reparación?

Dependiendo del daño se realiza la reparación, si el daño es pequeño como falla de un cable de red dañado se lo repara de inmediato pero si el daño es mayor se tarda un poco más.

¿Se realiza mantenimiento periódicamente de hardware y software en la Universidad?

Cabe recalcar que no todos los equipos de la Universidad se encuentran bajo la responsabilidad de la DITIC. El mantenimiento de software se lo realiza de acuerdo a la demanda o según la necesidad o requerimientos del usuario. El mantenimiento de hardware se lo realiza únicamente cuando sucede un problema, es decir se realiza un mantenimiento correctivo.

¿La Universidad cuenta con controles contra software malicioso?

Si, la Universidad cuenta con la licencia de Kaspersky Anti-Virus para los diferentes equipos, este se lo instala mediante un agente de red el cual a su vez permite realizar un monitoreo de los equipos que se encuentran conectados a la red y las amenazas si existiere.

¿Se cuenta con manuales de procedimientos para la obtención de backups de los archivos de datos y programas?

No, no se cuenta con ningún manual de procedimientos implementados, la Dirección se está reestructurando y anteriormente no se contaba con ningún manual, se planifica que con la reestructuración actual se siga implementando los diversos manuales.

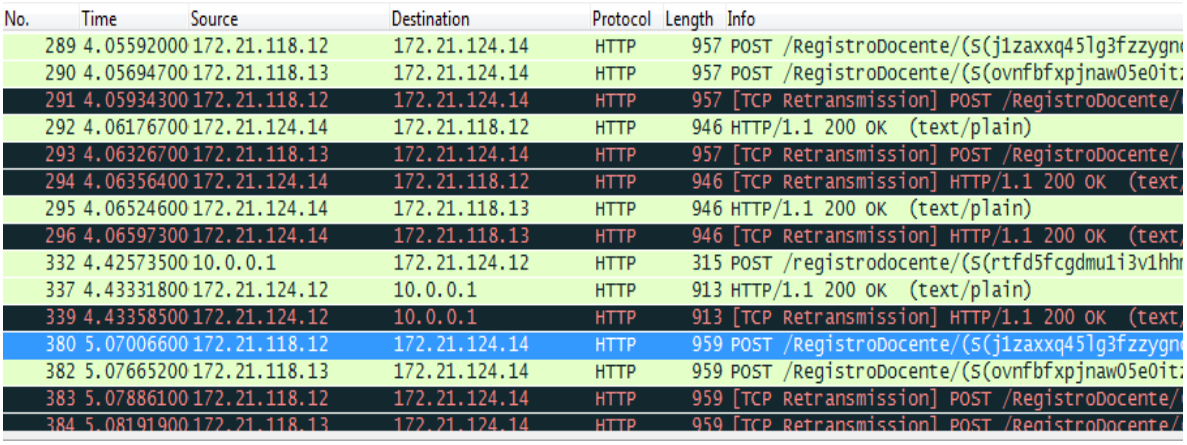
Con la información recolectada en la entrevista se puede definir que la UTA se encuentra expuesta a ataques internos o externos. La falta de controles y políticas de seguridad de la información en una institución la hace vulnerable a diversos ataques, por tal motivo se llega a la conclusión de que la universidad requiere establecer políticas de seguridad ya que estas son una línea base para controlar y proteger los activos de la Universidad.

4.1.6. Análisis de vulnerabilidades

Para detectar vulnerabilidades en la red de la Universidad Técnica de Ambato, se utilizó la herramienta W*ireshark* que sirve como analizador de protocolos, utilizado por algunos profesionales para resolver problemas en la red, examinar problemas de seguridad, depurar la implementación de protocolos y los estudiantes lo usan para aprender el funcionamiento interno de la red.

Se realizó un análisis a la red inalámbrica de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial FISEI se encontró los siguientes paquetes del protocolo HTTP capturados, como se observa en el Gráfico Nº 5, se muestra información como número de Frame, tiempo en segundos de la captura, la dirección IP de origen, la IP destino, el protocolo

involucrado, el tamaño del paquete y finalmente información adicional que Wireshark previamente decodificado.



No.	Time	Source	Destination	Protocol	Length	Info
289	4.05592000	172.21.118.12	172.21.124.14	HTTP	957	POST /RegistroDocente/(S(j1zaxxq45lg3fzzygn
290	4.05694700	172.21.118.13	172.21.124.14	HTTP	957	POST /RegistroDocente/(S(ovnfbfxpjnaw05e0it
291	4.05934300	172.21.118.12	172.21.124.14	HTTP	957	[TCP Retransmission] POST /RegistroDocente/
292	4.06176700	172.21.124.14	172.21.118.12	HTTP	946	HTTP/1.1 200 OK (text/plain)
293	4.06326700	172.21.118.13	172.21.124.14	HTTP	957	[TCP Retransmission] POST /RegistroDocente/
294	4.06356400	172.21.124.14	172.21.118.12	HTTP	946	[TCP Retransmission] HTTP/1.1 200 OK (text
295	4.06524600	172.21.124.14	172.21.118.13	HTTP	946	HTTP/1.1 200 OK (text/plain)
296	4.06597300	172.21.124.14	172.21.118.13	HTTP	946	[TCP Retransmission] HTTP/1.1 200 OK (text
332	4.42573500	10.0.0.1	172.21.124.12	HTTP	315	POST /registrodocente/(S(rtfd5fcgdmu1i3v1hh
337	4.43331800	172.21.124.12	10.0.0.1	HTTP	913	HTTP/1.1 200 OK (text/plain)
339	4.43358500	172.21.124.12	10.0.0.1	HTTP	913	[TCP Retransmission] HTTP/1.1 200 OK (text
380	5.07006600	172.21.118.12	172.21.124.14	HTTP	959	POST /RegistroDocente/(S(j1zaxxq45lg3fzzygn
382	5.07665200	172.21.118.13	172.21.124.14	HTTP	959	POST /RegistroDocente/(S(ovnfbfxpjnaw05e0it
383	5.07886100	172.21.118.12	172.21.124.14	HTTP	959	[TCP Retransmission] POST /RegistroDocente/
384	5.08191900	172.21.118.13	172.21.124.14	HTTP	959	[TCP Retransmission] POST /RegistroDocente/

Gráfico Nº 5: Captura de trafico de red con Wireshark.

Elaborado por: Elizabeth Torres

Luego de capturar los paquetes se analizó uno de los paquetes capturados, como se muestra en el Gráfico N° 6 la primera zona muestra los datos del Frame capturado, nos da información de todos los protocolos involucrados en la captura. A continuación Ethernet II que nos muestra la cabecera Ethernet II que a su vez pertenece a la capa de enlace de datos, muestra información como la dirección MAC Origen, dirección MAC Destino y el tipo protocolo que viaja en la parte de datos de la trama. Luego vemos Internet Protocol con los datos de la cabecera del datagrama IP. Después nos encontramos con Transmission Control Protocol, se trata del Segmento TCP, con información de puerto de origen, puerto destino, número de secuencia.

Posteriormente, el Hipertext Transfer Protocol, donde se muestra información de le método, la dirección URL a donde se hizo la petición, la versión, el navegador utilizado, el lenguaje utilizado etc. En el Grafico N° 6 se muestra toda la información capturada por el paquete HTTP.

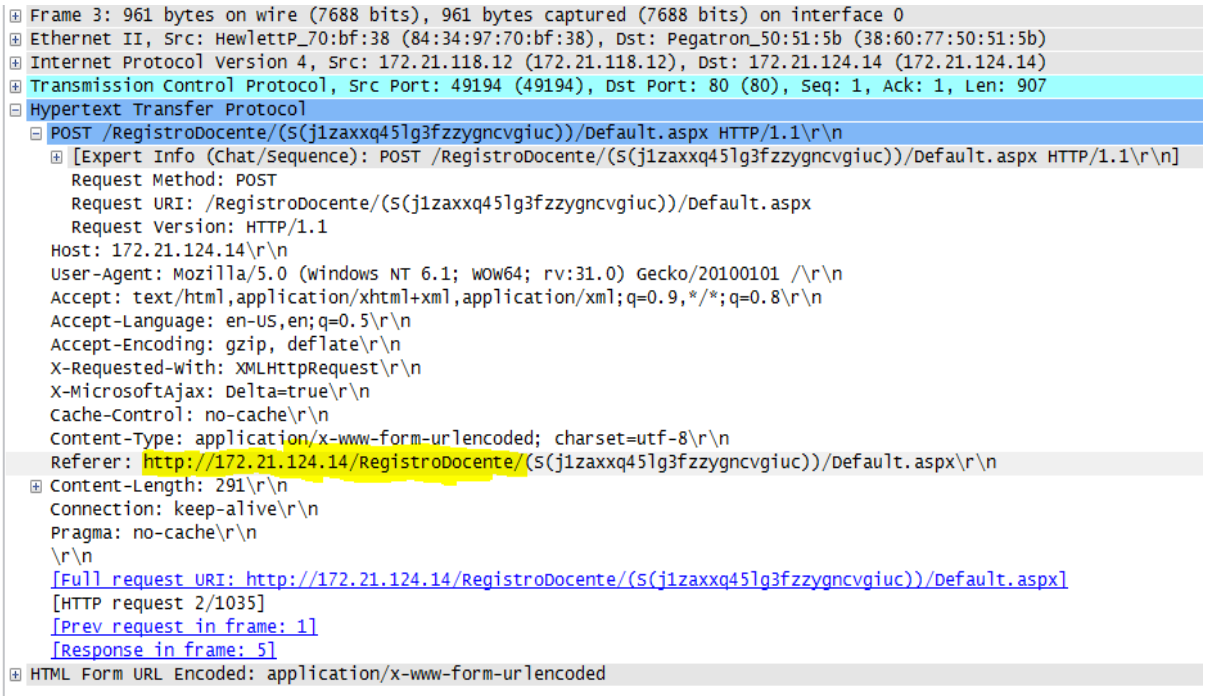


Gráfico Nº 6: Paquete Http.

Elaborado por: Elizabeth Torres

Una de las vulnerabilidades encontradas fue que, mediante la captura de paquetes se puede obtener la dirección IP de los servidores y los puertos por los que se realizan las peticiones, en la captura anterior podemos observar que para el registro de actividades de los docentes se utiliza la http://172.21.124.14/RegistroDocente/Default.aspx, se conoce que el registro se lo realiza con el número de cedula del docente. Entonces conociendo la dirección IP de la aplicación, con herramientas más especializadas se puede realizar un ataque de denegación de servicio.

Además en el análisis realizado se puede observar que se muestra el nombre del servicio para el registro de los docentes, en que gestor fue desarrollado en este caso ASP.NET y por ende la versión.

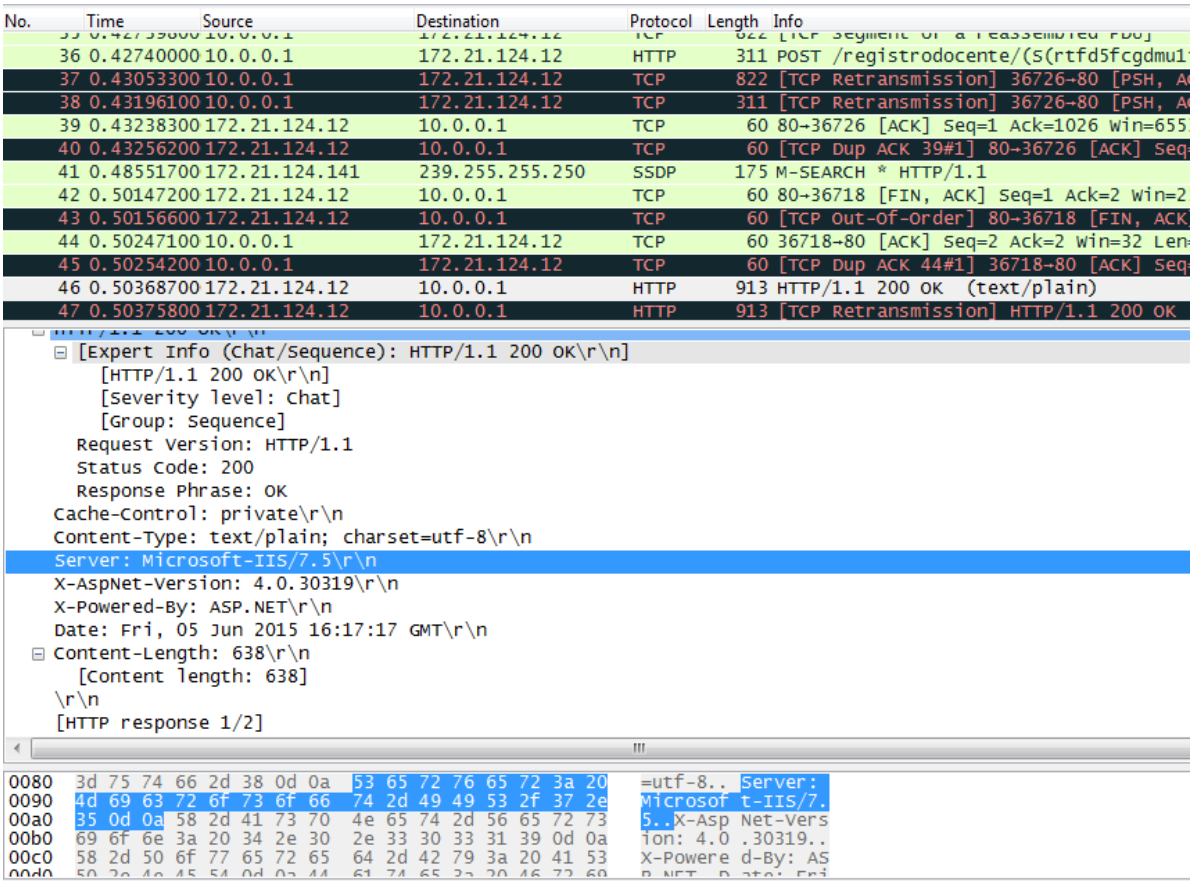


Gráfico Nº 7: Salida de un paquete capturado.

Elaborado por: Elizabeth Torres

4.2. Establecimiento de lineamientos de seguridad de la información mediante parámetros de la norma ISO/IEC 27002:2013

4.2.1. Desarrollo de políticas de seguridad

La gran diversidad de amenazas internas y externas a las que está sometida la información son conocidas, la política de seguridad busca minimizar los riesgos, el éxito total se conseguirá con el compromiso de las autoridades de la universidad, con la difusión completa y extensa de las políticas y con el compromiso masivo de los usuarios en el cumplimiento total de las políticas.

El desarrollo de las políticas de seguridad de la información se realizó en la DITIC de la UTA, partiendo de la información recopilada del análisis de la situación actual y basándose en los controles de la norma ISO 27002 en su versión 2013.

4.2.2. Políticas de seguridad

El presente dominio tiene por objetivo establecer los lineamientos iniciales para la creación de políticas de seguridad de la información, las mismas que ayudarán a preservar las tres principales características de la información como son integridad, confidencialidad y disponibilidad de la información [13]. Las políticas establecidas en el presente dominio se basan en los objetivos establecidos en el Portal de ISO, "Políticas de Seguridad" [16].

- Directrices de la dirección en seguridad de la información.

  - Conjunto de políticas para la seguridad de la información.

Crear un manual de roles y responsabilidades para cada uno de los funcionarios, se debe establecer como política de seguridad, el mismo que debe estar aprobado, publicado y comunicado a todos los empleados de la universidad.

Para el cumplimiento de esta política es necesario que la DITIC asigne un comité para la creación del manual de roles, políticas y responsabilidades para cada uno de los funcionarios, el mismo que debe ser documentado, revisado, verificado, y aprobado por la máxima autoridad de la Dirección y Universidad, tomando en cuenta todos los cargos concernientes a políticas de seguridad de la información. En este manual deben constar todos los cargos, que se encuentran detallados en el organigrama de la Dirección.

- Revisión de las políticas para la seguridad de la información.

En lo que corresponde a revisión de políticas de seguridad se debe realizar periódicamente, al igual que el manual de roles y responsabilidades asignados a los funcionarios o al realizarse un cambio dentro de la universidad.

Para el cumplimiento de esta política es necesario que DITIC de la UTA asigne un comité interno o externo para la revisión del manual de roles, políticas y responsabilidades asignadas a los diferentes cargos de la dirección, este manual debe detallar las responsabilidades y procedimientos necesarios para mantener segura la información. Además se debe tomar en cuenta los siguientes servicios:

Servicios para la docencia

La DITIC debe asegurar el buen funcionamiento de los equipos computacionales de los docentes y estudiantes. Así como brindar mantenimiento de los equipos de cómputos, asistencia técnica para la adquisición de nuevos equipos tecnológicos en todas las unidades administrativas y facultades. Además de asegurar el correcto funcionamiento del sistema Utamático.

Servicios para la administración

La DITIC debe garantizar que una vez adquiridos los requerimientos de las áreas administrativas y técnicas: el análisis, diseño y desarrollo de los sistemas para la gestión; sean eficientes, para que la parte administrativa cuente con los sistemas necesarios, asegurando el correcto funcionamiento de los diferentes procesos de la universidad. Además de brindar soporte técnico y logístico en sistemas informáticos y diseño, administración y actualización de la página web de la UTA.

Servicios institucionales

La DITIC debe optimizar el flujo y manejo de datos, mediante la correcta administración de la red de comunicación y de la red inalámbrica interna de la universidad con el uso de nuevas tecnologías.

Una de las principales debilidades detectadas es que no se cuenta con las responsabilidades y procedimientos, en lo que se refiere a seguridad de la información.

4.2.3. Aspectos organizativos de la seguridad de la información

Una de las partes fundamentales de los objetivos y actividades de la universidad es la administración de la seguridad de la información [14], para ello lo primordial es la gestión, para realizar tareas como la aprobación, implementación y asignación de procedimientos y responsabilidades de políticas de seguridad. Para un desenvolvimiento exitoso en aspectos de seguridad se debe tener un asesoramiento externo sobre seguridad de la información. Las políticas establecidas en el presente dominio se basan en los objetivos expuestos en el portal de ISO, "Aspectos organizativos de la seguridad de la información" [17].

- Organización interna

  - Asignación de responsabilidades para la seguridad de la información.

Se establece como política de seguridad definir y documentar las responsabilidades de los funcionarios de la DITIC, en especial las que tienen que ver con seguridad de la información.

Para el cumplimiento de esta política es necesario que la persona responsable de la DITIC de la UTA asigne un responsable para elaborar el manual de políticas y procedimientos para el área de tecnologías de la información y comunicación en el que se debe plasmar los

diversos roles y responsabilidades, con énfasis principal a los cargos concernientes a seguridad de la información. Las debilidades detectadas son:

- ✓ Actualmente la universidad no cuenta con personas dedicadas a la seguridad de la información.
- ✓ No poseen un manual de respaldos de la información, pero si realizan un respaldo diario de los sistemas y bases de datos.
- ✓ No disponen de un listado de amenazas de activo de información.
- ✓ No generan manuales de configuración de los diversos sistemas, ni planes de contingencia antidesastres.

- Segregación de tareas.

La política de seguridad es segregar tareas y áreas de responsabilidad para cada uno de los miembros o funcionarios de la dirección para evitar modificaciones no autorizadas o no intencionadas.

Para el cumplimiento de esta política es necesario que cada funcionario o encargado del área de sistemas de cada departamento o facultad capacite a los usuarios de su área o departamento asignado a su responsabilidad, sobre el uso de los sistemas de información y bases de datos si fuera el caso, para evitar modificación no autorizada o no intencionada, o el mal uso de los activos. De ocurrir algún conflicto el responsable del departamento o área será el encargado de solucionarlo.

En caso de ocurrir incidentes relacionados con áreas seguras como perímetros de seguridad, control de acceso, protección contra amenazas externas y de medio ambiente que el encargado del departamento o facultad no pueda solucionarlo deben notificar al encargado de Seguridad de la Información.

- Contacto con las autoridades.

Mantener el contacto con las autoridades institucionales o nacionales apropiadas que rijan la Educación Superior para mantenerse actualizados ante posibles cambios en los reglamentos o leyes.

Para el cumplimiento de esta política es necesario que se mantenga contacto con autoridades de universidades de la provincia y nacionales para brindar un mejor rendimiento dentro de la institución, en caso de realizarse alguna actualización en las políticas de uso de la información.

Además al mantener contacto con las autoridades pertinentes dentro de la universidad es importante para la aprobación y revisión de las políticas y procedimientos que se agreguen dentro de la universidad.

- Contacto con grupos de interés especial.

La política de seguridad es mantener contacto con especialistas de seguridad de la información ya sea mediante grupos o foros.

Para el cumplimiento de esta política es necesario que una persona se mantenga actualizada sobre seguridad de la información, debe estar agregada a foros o grupos de especialistas de seguridad de la información para tener información sobre cambios o actualizaciones de las políticas de seguridad de la información.

- Seguridad de la información en la gestión de proyectos.

Para la seguridad de la información en la gestión de proyectos la política de seguridad es implementar procedimientos de control de la información en la gestión y desarrollo de proyectos dentro de la universidad.

Para el cumplimiento de esta política es necesario que al gestionar y desarrollar nuevos proyectos dentro de la universidad, sin importar la índole del proyecto se aplique políticas de seguridad, es necesario que todo proyecto sea comunicado a la dirección para determinar que políticas se aplican a dicho proyecto.

Se debe asignar una comisión para que realice un análisis sobre la información a utilizar en el proyecto y para determinar las políticas a utilizar.

- Dispositivos para movilidad y teletrabajo

  - Política de uso de dispositivos para movilidad.

La política de seguridad es adoptar medidas de seguridad para manipulación de datos mediante dispositivos de movilidad.

Para el cumplimiento de esta política es necesario que la red de datos para dispositivos móviles sea restringida por control de acceso a redes, además que se debe controlar las aplicaciones o sistemas de información que se puedan ingresar desde dispositivos móviles. Se debe tomar en cuenta el control de acceso y la virtualización de las redes.

  - Teletrabajo.

La política de seguridad es proteger la información a la que accede, procesa o almacena él o los funcionarios, desde ubicaciones distintas a su puesto de trabajo.

Para el cumplimiento de esta política es necesario realizar protección lógica de los equipos, que únicamente el personal autorizado por el responsable de seguridad de la información podrá ingresar a realizar cambios o trabajo fuera de la oficina. En caso de ocurrir fallas en la red deberá ingresar mediante los puertos de configuración, los que únicamente personal

autorizado debe conocer las claves de acceso. Además proteger mediante la utilización de contraseñas de acceso tanto a acceso remoto como a los puertos de configuración de servidores.

4.2.4. Seguridad ligada a los recursos humanos

El presente dominio pretende educar e informar a los funcionarios y colaboradores de la universidad desde que ingresan y de forma continua sobre la prioridad de preservar la confidencialidad de la información que se maneja, las sanciones a las que se encuentra expuesto en caso de incumplimiento de alguna política de seguridad. Además de que la universidad deposita toda su confianza al entregarle el acceso a información, por ende el funcionario debe estar cociente de la importancia y responsabilidad que tiene a su cargo. Las políticas establecidas en el presente dominio se basan en los objetivos expuestos en el Portal de ISO, "Seguridad ligada a los recursos humanos" [18].

- Antes de la contratación

  - Investigación de antecedentes.

Para los aspirantes a cargos administrativos o docentes para la universidad, es necesario realizar una investigación previa de antecedentes e historial laboral, para descartar todo tipo de amenaza a la seguridad de la universidad y de la información.

Para cumplir con esta política se debe realizar pruebas de admisión, pedir referencias personales, laborares, record del aspirante que asegure no tener problemas de índole legal. Además se debe consideras las siguientes verificaciones:

- ✓ Referencias satisfactorias ya sea personales, institucionales o comerciales.
- ✓ Chequeo de currículo vitae, historial laboral.
- ✓ Revisión de calificaciones académicas y profesionales obtenidas anteriormente.

- ✓ Chequeo de documentos de identificación personal.
  - Términos y condiciones de contratación.

Luego de la selección del nuevo funcionario en el cargo que sea, debe existir un contrato firmado y/o legalizado, el que debe incluir cláusulas de confidencialidad, y las obligaciones en materia de seguridad de la información, las que el funcionario debe cumplir ya sea persona natural o jurídica.

La política de seguridad es que como parte del contrato debe incluirse una clausula en la cual acepta los términos y condiciones, que le obligan al funcionario a declararse como responsable de dar cumplimento a las políticas de seguridad que sean aplicables.

- ✓ Todo el personal administrativo, de servicio y docente que tenga acceso a información sensible, debe firmar un acuerdo de confidencialidad, antes de otorgarle el acceso a los medios de información.
- ✓ Aceptación de las responsabilidades y derechos de ser auditados cuando la universidad lo requiera.
- ✓ Aceptación de la responsabilidad de clasificar la información, la gestión de activos organizacionales de los diversos sistemas internos y externos asociados a la universidad.
- ✓ Aceptación de las responsabilidades de manejar información recibida, de compañías o partes externas, e información personal de los empleados creada durante el transcurso del empleo en la organización.
- ✓ Las acciones a las que está expuesto el empleado en caso de no cumplir con los requerimientos de seguridad.

Para el cumplimiento de esta política se puede descargar un ejemplo de “Acuerdo de Confidencialidad” [16].

- Durante la contratación

  - Responsabilidades de gestión.

La política de seguridad es incluir todos los términos y condiciones de seguridad de la información cuando se realice el contrato con empleados, contratistas y terceros para la gestión de las mismas.

Para el cumplimiento de esta política es necesario que los términos y condiciones esten incluidas en el contrato de trabajo, estableciendo las diversas responsabilidades del empleado en la seguridad de la información. Los empleados deben estar informados adecuadamente sobre los roles y responsabilidades de seguridad, además de las sanciones en caso de incumplimiento, cuando la información este bajo su responsabilidad.

  - Concienciación, educación y capacitación de seguridad de la información.

La política es incluir capacitaciones y requerimientos de seguridad, al asignar responsabilidades a cada funcionario, al iniciar y durante las labores. El responsable de coordinar las labores de capacitación necesarias para difundir las políticas de seguridad, es el departamento de talento humano en coordinación con la DITIC.

Todo el personal administrativo y docente debe recibir una adecuada capacitación y actualización sobre las políticas y normas relacionadas a la seguridad institucional y de la información.

Dentro de la DITIC, el área de seguridad de la información es la encargada de proporcionar el material necesario para la capacitación, dicho material debe ser actualizado cada seis meses o cada vez que sea necesaria a fin de que la información ahí reflejada sea precisa.

- Proceso disciplinario.

En cuanto al proceso disciplinario, la política es que todos los incumplimientos u omisiones según la gravedad del acto, deben ser sancionados según políticas administrativas internas vigentes en la UTA.

Para el cumplimiento de esta política, cualquier proceso disciplinario debe iniciarse cuando se haya verificado que se ha producido una violación a la seguridad de la información, este proceso debe garantizar el trato justo y correcto para la universidad y los empleados.

El proceso debe pronosticar una respuesta gradual, tomando en consideración la gravedad del acto, su impacto en la universidad, si el empleado fue correctamente capacitado, la sanción debe estar basada en el acuerdo de confidencial firmado al iniciar el contrato. Dependiendo de la gravedad del acto, el proceso deberá permitir la remoción inmediata de los derechos de acceso y privilegios otorgados, o la separación inmediata del empleado de la universidad.

 Cese o cambio de puesto de trabajo

- Cese o cambio de puesto de trabajo

La política de seguridad es incluir la comunicación de las responsabilidades a la terminación de las actividades, los términos y condiciones incluidos en el contrato y acuerdo de confidencialidad. El funcionario administrativo o docente debe presentar su renuncia de cese de funciones con suficiente tiempo de antelación, por lo menos 15 días de anticipación.

El encargado del área donde el empleado realizó sus funciones, es el responsable de supervisar la entrega formal de los activos al nuevo funcionario a ocupar la vacante, esto incluye claves de acceso, documentación, llaves, credenciales, herramientas de trabajo, equipos de cómputo y demás activos a su cargo.

El área de seguridad de la información es la encargada de inhabilitar las claves de acceso a los diversos sistemas de información, acceso a central de datos, acceso a bases de datos y correo electrónico del empleado que deja de pertenecer a la universidad. De ser necesario cambiar las claves de acceso a todos los sistemas de información que sean vulnerables a acceso.

4.2.5. Gestión de activos

Este dominio tiene por objetivo que la universidad tenga conocimiento de todos los activos que posee, que son importantes para administrar los diversos procesos que se realizan dentro de esta. Incluyendo los activos informáticos que son base de datos y archivos, procedimientos, manuales, planes de contingencia y de continuidad, documentación de archivos; activos de software como aplicaciones, sistemas de información, utilitarios y herramientas; los activos físicos son equipos de administración, comunicación y de uso de estudiantes, medios magnéticos, equipos técnicos y activos en cuanto a servicios informáticos de comunicación y utilitarios. Las políticas de seguridad desarrolladas en este dominio proyectan cumplir con los objetivos de control planteados en el portal ISO, "Gestión de activos" [19].

- Responsabilidad sobre los activos

  - Inventario de Activos

Como política de seguridad la DITIC debe tener identificados los activos de información, en especial los más importantes y la relación con los sistemas de información que maneja la universidad, así como sus respectivos custodios y la ubicación física de cada activo.

Se verificó que la UTA cuenta con el departamento de administración de bienes el que está a cargo de realizar el inventario de activos de cada departamento, dirección y facultad.

El inventario de activos debe estar actualizado permanentemente, en caso de que exista alguna modificación administrativa o de estado del activo, en caso de que sucediera un cambio en el activo y este no se notificaría al departamento de administración de bienes o la DITIC dependiendo del activo, la responsabilidad recaerá sobre el custodio del activo.

La importancia de contar con un inventario de activos dentro de la UTA es para que se cumplan los objetivos propuestos dentro de la DITIC. El activo esencial es la información que manejan los sistemas, los mismos que son necesarios para brindar servicios a los estudiantes, docentes y personal administrativo, además de que son indispensables para que funcionen las aplicaciones.

Los equipos informáticos ayudan a hospedar los datos, los dispositivos de red ayudan a intercambiar información, las instalaciones que amparan equipos informáticos y de comunicaciones, son activos importantes para las diversas operaciones dentro de la universidad, es por esta razón todos estos activos deben estar inventariados.

- Propiedad de los Activos

En cuanto a propiedad de activos, la política es que toda la información que pertenezca a la universidad está sujeta a revisiones periódicas por parte del área de seguridad de la información por la persona asignada para esta función.

Los activos de información pertenecen a la UTA, a menos que las leyes nacionales dicten lo contrario, por esta razón la facultad de otorgar acceso a la información es el Área de Seguridad, área encargada de resguardar la seguridad de los datos.

Para cumplir esta política, cada uno de los activos de la información como hardware, software, equipos de cómputo, de comunicaciones y la información deben estar custodiadas

por un funcionario a cargo de actividades relacionadas con dicho activo. Con esta relación se crea una responsabilidad sobre el uso del activo. Como se muestra en la Tabla Nº 2.

PROPIETARIOS DE LA INFORMACIÓN		
INFORMACIÓN	PROPIETARIO	PROCESOS INVOLUCRADOS
Financiera Contable	Departamento financiero	Controles contables.
		Estrategias financieras.
		Auditorias contables y financieras.
		Controles y auditorias tributarias.
		Control de pagos.
Académica	Secretaria de Facultades	Matriculas a estudiantes.
		Controles académicos estudiantiles.
	Coordinadores de Carreras	Asignación de estudiantes a cursos.
		Elaboración de distributivos.
		Elaboración de horarios para docentes y cursos.
Nomina	Dirección de Talento Humano	Contrato a docentes.
		Control de asistencia de personal administrativo y docente.
		Evaluación al desempeño de los docentes.
Inventarios	Administrativo	Control de inventarios.
		Control de activos fijos.
		Designación de custodios de activos.

Tabla Nº2.- Responsabilidades sobre uso de activos

Elaborado por: Elizabeth Torres

- Uso aceptable de los activos

La política se rige en que los activos de información de la UTA son de propiedad de la misma, por tal motivo debe ser utilizada únicamente para fines laborales, para cumplir a cabalidad

con esta política se debe tomar en cuenta la siguiente tabla para y seguir los siguientes lineamientos:

	Computadores Personales		**Computadores Portátiles**		**Computadores Propiedad de terceros**	
Lineamiento	**SI**	**NO**	**SI**	**NO**	**SI**	**NO**
Toda modificación debe ser autorizada por el Área de Seguridad de la Información.	x		x			x
La instalación, desinstalación o mantenimiento de equipos le debe realizar personal del área de Sistemas.	x		x			x
Inventario competo de hardware y software. (Anexo A)	x		x			x
Lineamientos de uso de los equipos. (Anexo A)	x		x			x
Los equipos son de uso exclusivo para desarrollar actividades relacionadas con la Universidad.	x		x			x
Los equipos deberán permanecer dentro de las instalaciones de la Universidad.	x		x			x
Los equipos portátiles solo pueden salir de la universidad bajo responsabilidad total del custodio asignado.		x	x			x
Si el responsable del equipo no se encuentra en la Universidad, el equipo asignado a su cargo no puede salir de las instalaciones.		x	x			x
Utilizar aplicaciones necesarias para el desarrollo de las funciones asignadas.	x		x		x	
Instalación de software autorizado y licenciado por el Área de Seguridad de la Información.					x	
Mantener actualizadas las aplicaciones.					x	

Mantener actualizado y activo el antivirus.	x		x		x	
Mantener una clave de acceso al equipo para evitar el acceso no autorizado.			x		x	

Tabla Nº3.- Lineamientos uso aceptable de activos

Elaborado por: Elizabeth Torres

Lineamientos de seguridad de la información:

- ✓ Los recursos de la uta como internet, correo electrónico y sistemas de información, podrán ser usados para fines laborales, caso contrario únicamente bajo autorización del área de seguridad de la información.
- ✓ La jefatura de cada departamento es el responsable directo de asignar las tareas a cada empleado del departamento, y el nivel de acceso a la información mediante la asignación de roles.
- ✓ Está estrictamente prohibido la divulgación de la información almacenada, creada o transmitida por los sistemas de Información de la UTA.
- ✓ Las aplicaciones, software y sistemas de información que utiliza la universidad deben tener vigente su licencia, los mismos que deben ser instalados por personal del área de sistemas.
- ✓ Al área de seguridad de la información es la responsable de la creación de cuentas de usuario, incluyendo los mecanismos de seguridad como contraseñas, control de acceso a centrales de datos, auditorias de base de datos, monitoreo de uso de los sistemas; mecanismos que aseguren la integridad de los datos mediante la red cableada e inalámbrica.
- ✓ Está terminantemente prohibido compartir el usuario y contraseñas, e información confidencial a terceras personas o entidades externas, ya sea por correo electrónico u cualquier medio físico.
- ✓ Los sistemas de información, correo y computadores de propiedad de la universidad están sujetos a ser auditadas por personal del Área de Seguridad cuando sea necesario, caso contrario una vez al año.

- ✓ La universidad es responsable de brindar al empleado los recursos necesarios para realizar su trabajo, así como verificar que servicio de internet y correo electrónico se encuentren en perfecto funcionamiento. El área de sistemas es responsable de implementar controles como firewall, antivirus, IPS/IDS, etc. para asegurar que la información almacenada se encuentre protegida.
- ✓ La universidad está en todo el derecho de revocar los privilegios de uso de activos de la información, emisión de sanciones e incluso trámites legales al usuario que ponga en riesgo la integridad, confiabilidad y disponibilidad de la información, los equipos y sistemas de información.
- ✓ El uso de internet y correo electrónico dentro de la universidad será únicamente para actividades en beneficio de la institución, nunca con fines de lucro o actividades personales.
- ✓ Queda prohibido el ingreso a sitios de dudosa procedencia, hacking, pornografía o contenido no apropiado para los estudiantes, administrativos o autoridades.
- ✓ Realizar monitoreo permanente sobre el acceso a internet y correo electrónico institucional de los miembros de la universidad.
- ✓ Se establecen restricciones de acceso a redes inalámbricas, de acuerdo a las necesidades de cada facultad o departamento.
- ✓ Para crear cuentas de correo electrónico se debe evitar utilizar caracteres especiales, la dirección de correo debe ser representativo al usuario, se asignará un tamaño de almacenamiento para el buzón de correo.
- ✓ Al enviar un correo electrónico se lo debe hacer desde la cuenta de correo de la persona que lo firma, deben tener características básicas de cordialidad y respeto, cortas y concisas, en el asunto siempre debe ir una frase que haga referencia al contenido del correo.
- ✓ Queda prohibido él envió de mensajes en cadenas o similares, el incumplimiento causaría la suspensión del servicio temporal o definitivo.

- Devolución de activos

Durante el proceso se cesación de funciones la política de seguridad es garantizar que se cumpla con la entrega formal de los activos a cago del funcionario, para el cumplimiento de la política se toma en cuenta los siguientes lineamientos:

- ✓ Devolución de equipos completos, es decir, software, manuales y herramientas de trabajo.
- ✓ Activos organizacionales, equipos móviles, claves de acceso, medios de almacenamiento.
- ✓ Toda la información de la universidad que se encuentre en el equipo personal del funcionario, debe ser transmitida a la institución y removida de forma permanente del equipo.
- ✓ Si el empleado posee información sobre tareas tecnológicas o administrativas relacionadas con su labor dentro de la institución, debe transmitir todo su conocimiento mediante documentación a la universidad.

- Clasificación de la información

- Directrices de clasificación

La política de seguridad es clasificar la información de acuerdo a las tres características de seguridad: confidencialidad, integridad y disponibilidad. A continuación se muestra la clasificación considera de acuerdo a las características mencionadas.

Por Confidencialidad

Nivel 0	Información de acceso público, no confidencial.
Nivel 1	Información de acceso privado e interno. Uso interno destinada a personal interno y cuya divulgación podría crear riesgos leves para la Universidad.
Nivel 2	Información considerada como confidencial, utilizada por un grupo autorizado de funcionarios, su divulgación provocaría pérdidas significativas para la Universidad.
Nivel 3	Información considerada como estrictamente confidencial, utilizada por un grupo específico de funcionarios, directivos y autoridades, su divulgación provocaría pérdidas graves para la Universidad.

Tabla Nº 4.- Clasificación de la información según nivel de Confidencialidad

Elaborado por: Elizabeth Torres

Por Integridad

Nivel 0	Información que al modificarse puede ser rectificada fácilmente.
Nivel 1	Información que al modificarse puede ser rectificada pero ocasiona pérdidas leves para la Universidad.
Nivel 2	Información que al modificarse es difícil corregir y ocasiona daños y pérdidas significativas para la Universidad.
Nivel 3	Información que al modificarse no puede ser corregida y ocasiona pérdidas graves o cuantiosas para la Universidad.

Tabla Nº 5.- Clasificación de la información según nivel de Integridad

Elaborado por: Elizabeth Torres

Por Disponibilidad

Nivel 0	Información que no afecta las operaciones de la Universidad si no está disponible.
Nivel 1	Información que al no estar disponible durante una semana, puede afectar levemente las operaciones de la Universidad.
Nivel 2	Información que al no estar disponible durante 24 horas puede afectar significativamente en las operaciones de la Universidad.
Nivel 3	Información que al no estar disponible durante 1 hora puede afectar significativamente en las operaciones de la Universidad.

Tabla Nº 6.- Clasificación de la información según nivel de Confidencialidad

Elaborado por: Elizabeth Torres

A todo tipo de información de la universidad debe asignarle un valor por cada criterio, basándose en la siguiente tabla:

ACTIVO	Confidencialidad	Disponibilidad	Integridad
Información de estudiantes	1	1	2
Información de Docentes	1	1	1

Tabla Nº 7.- Valorización de la información

Elaborado por: Elizabeth Torres

Después de asignar el valor de acuerdo a los diferentes niveles, se debe asignar una clasificación de criticidad de acuerdo a la siguiente tabla:

Criticidad Baja	Todos los valores dentro del nivel 0 y 1
Criticidad Media	Valores del nivel 2
Criticidad Alta	Valores del nivel 3

Tabla Nº 8.- Clasificación de la información según nivel de Criticidad

Elaborada por: Elizabeth Torres

Se debe clasificar la información almacenada en medios físicos, utilizando etiquetas para establecer el nivel de criticidad, y capacitar a los funcionarios que la manipula para evitar hurto de información o manipulación inadecuada o eliminación de información importante para la universidad.

- Etiquetado y manipulado de la información

En lo que se refiere al etiquetado y manipulación la política de seguridad es etiquetar la información y los activos, para que los funcionarios sepan cómo manipularlos y evitar perdida, manipulación o hurto de información esencial.

Para el cumplimiento de esta política, la forma de etiquetar la información se lo debe hacer mediante el uso de colores, para simular un semáforo de acuerdo al nivel de criticidad, como se detalla en la siguiente tabla:

Criticidad Baja	Todos los valores dentro del nivel 0 y 1	Verde
Criticidad Media	Valores del nivel 2	Amarilla
Criticidad Alta	Valores del nivel 3	Roja

Tabla Nº 9.- Clasificación de la información según nivel de Criticidad

Elaborada por: Elizabeth Torres

De acuerdo a la tabla anterior de debe marcar e identificar la información que se maneja dentro de la universidad, para definir los controles de seguridad que se debe dar a cada una.

- Manipulación de activos

En referencia a la manipulación de activos, la política de seguridad es que todos los funcionarios que utilizan activos de información, deben tener conocimiento de los niveles de criticidad y las políticas de seguridad que debe cumplir para manipular la información.

Para el cumplimiento de esta política es necesario que al momento que ingresa un nuevo empleado a la universidad, se realizase una capacitación sobre los niveles de criticidad de la información a la que va a acceder, además de compartir las políticas de seguridad que debe aplicar, para evitar errores en la manipulación de activos de información. Mantener constantemente capacitados a todo el personal de la universidad sobre las nuevas políticas o niveles de criticidad de la información.

- Manejo de los soportes de almacenamiento

  - Gestión de soporte extraíbles.

Para la gestión de soporte extraíbles la política de seguridad es que el responsable de cada área, departamento o facultad dependiendo de la criticidad de la información que ahí se procese, controlar los medios informáticos removibles que ahí se utilicen.

Para el cumplimiento de esta política es necesario que los medios informáticos removibles que existan en cada departamento, debe estar asignado para cada proceso o para almacenar determinada información, por ejemplo se debe asignar solo un disco duro para guardar los respaldos de información, y no utilizarlo para otro fin.

  - Eliminación de soportes.

En lo que se refiere a eliminación de soporte la política de seguridad es eliminar o expulsar los medios informáticos removibles de los equipos de forma segura, para evitar el plagio de información.

Para el cumplimiento de esta política es necesario que el encargado del área, departamento o facultad realice una revisión del medio informático al que se va a eliminar el soporte para verificar que se haya obtenidos los respaldos necesarios, y que no contenga información de la Universidad. Luego debe ser formateado para borrar toda la información que contenía.

- Soportes físicos en tránsito.

Como política de seguridad se propone proteger los medios de información contra acceso no autorizado cuando salgan del departamento o perímetro y seguridad.

Para el cumplimiento de esta política es necesario que la información que se encuentre en los medios removibles que salen fuera de la Universidad, sean protegidos por claves de acceso, o de lo contrario evitar que los medios removibles contenga información sensible o de alta criticidad para evitar el acceso no autorizado o la corrupción.

4.2.6. Control de acceso

Este dominio tiene por objetivo controlar el acceso a los sistemas de información, servicios de información, bases de datos e instalaciones de procesamiento de información por medio de restricciones de acceso y excepciones. Esto ayuda a mantener protegida la información, contra accesos no autorizados y manipulación inadecuada de información por personal ajeno a la Universidad. Las políticas de seguridad que se establecen en este dominio procuran cumplir con los controles establecidos en el Portal ISO, "Control de acceso" [20].

- Requisitos de negocio para el control de acceso.

- Política de control de acceso.

Como política de seguridad se propone, definir claramente los controles de derechos de acceso individual y grupal. Se debe tomar en cuenta los siguientes lineamientos:

- ✓ Definir los requerimientos de seguridad para las diversas aplicaciones y sistemas de la universidad.

- ✓ Identificar la información que debe ser protegida y está ligada a los sistemas de información.
- ✓ Velar por que se cumpla con las legislaciones y reglamentos vigentes, y que exista consistencia entre el nivel de acceso y el nivel de criticidad establecido.
- ✓ Identificar y definir niveles de acceso estándar para personal que cumpla con funciones básicas dentro de la universidad.
- ✓ Establecer un procedimiento para autorizar el acceso a los usuarios en ambientes simples y distribuidos.
- ✓ Si se delega la tarea de concesión de derechos de acceso, el jefe del área de seguridad de la información debe documentar y controlar a la persona asignada.
- ✓ Realizar un cronograma de revisión y auditoria de privilegios concedidos.
- ✓ Procedimientos para revocación de privilegios.
- ✓ Para obtener permisos de acceso se debe realizar una solicitud por escrito de la parte interesada, la misma que debe ser aprobada por la autoridad competente para que el administrador de base de datos habilite el acceso.

En el ANEXO B se encuentra el formulario de solicitud de acceso a los sistemas de información.

- Control de acceso a las redes y servidores asociados.

Para el control de acceso a redes y servidores, la política de seguridad es garantizar que los usuarios que tengan acceso a la red y a los servidores, no compliquen la seguridad de los mismos.

Para que esta política se cumpla a cabalidad el responsable del área de seguridad de la información es el encargado de brindar el acceso a los servidores, redes y recursos tecnológicos, los mismos que deben ser pedidos formalmente por el jefe departamental para cada funcionario a su cargo.

Las conexiones de acceso a la red y aplicaciones deberán ser especificadas como clasificadas o críticas, para los accesos desde áreas públicas que están fuera del control de seguridad de la institución o sitios de alto riesgo.

Este control está orientado a la activación y desactivación de los derechos de acceso a las redes de la Universidad, para lo cual se debe identificar cada una de las redes, los servicios y la accesibilidad a cada uno de ellos, además de determinar los usuarios y roles que se puede otorgar.

- Gestión de acceso de usuario

  - Gestión de altas/bajas en el registro de usuarios.

La política de seguridad es que el registro y cancelación de usuario, se debe realizar de manera independiente a cada usuario que requiera acceso a la información, este proceso está a cargo del área de seguridad de la información se debe tomar en cuenta los siguientes requerimientos:

- ✓ Realizar chequeos constantes de los usuarios que acceden a los servidores, sistemas de información y redes de datos, verificando que sean los autorizados por el área de seguridad de la información.
- ✓ Al crear un nuevo usuario debe contener un nombre único que identifique a que departamento pertenece, el usuario y el nivel de acceso asignado al funcionario para que realice las acciones que demanda su trabajo. Además se debe firmar el formulario del ANEXO C.
- ✓ Si el funcionario deja de pertenecer a la universidad deberá ser notificado de inmediato al área de seguridad de la información para realizar los cambios en el nivel de acceso del usuario.

En caso de incumplimiento de esta política el funcionario deberá ser sancionado de acuerdo a las políticas de la universidad.

- Gestión de los derechos de acceso asignados a usuarios.

Como política de seguridad se define implementar una herramienta o procedimientos para el control de usuarios, agregar o quitar permisos además de la gestión de las actividades realizadas por cada uno de ellos.

Es decir utilizar una herramienta que facilite el trabajo de una auditoria sobre los derechos de acceso asignados a cada usuario. Se recomienda utilizar herramientas *open source*, que faciliten la realización de auditorías, además de implementar procedimientos que ayuden a controlar que los permisos otorgados a los usuarios sean los que pueda realizar dentro de los sistemas de información.

- Gestión de los derechos de acceso con privilegios especiales.

Para la gestión de privilegios especiales, la política de seguridad es filtrar a los usuarios que requieran privilegios especiales a los sistemas de información, servidores, base de datos y servicios. Para cumplir con esta política se debe tomar en cuenta los siguientes lineamientos:

- ✓ Establecer por escrito y detalladamente los privilegios de acceso para los servidores, sistemas de información y bases de datos.
- ✓ Asignar privilegios de acceso y modificación únicamente a los módulos que sean necesarios para el cumplimiento de las funciones del usuario.
- ✓ Utilizar software para la asignación de privilegios los mismos que se asignaran a usuarios específicos.
- ✓ Mantener una revisión continua de las tareas realizadas por el usuario administrador de los sistemas de información.

- Gestión de información confidencial de autenticación de usuarios.

La política de seguridad es asignar contraseñas de acceso a los sistemas de información, previa autorización. Para cumplir con la política de seguridad se debe tomar en cuanto los siguientes lineamientos:

- ✓ Se debe firmar el formulario de creación de usuario y responsabilidad de contraseñas el que se puede encontrar en el ANEXO C.
- ✓ Asignar una clave temporal al usuario de modo que el usuario sea quien cree la clave pasando a ser confidencial e instransferible, de forma que ni el jefe del departamento tenga acceso.
- ✓ Para la asignación de una clave a un usuario se debe tener la autorización previa del jefe del departamento.
- ✓ La entrega de claves temporales se debe realizar en sobre sellado, adjunto a un documento de constancia de entrega de la clave y firma de recepción.
- ✓ Las contraseñas de servidores y sistemas se deben almacenar únicamente en mecanismos robustos de encriptación, no en equipos de cómputo comunes.
- ✓ Las claves otorgadas de fábrica a los equipos, deben ser cambiadas por claves complejas para asegurar su protección.
- ✓ Para los administradores de servidores, se debe entregar un listado de los servidores, usuarios y contraseñas para la administración previo autorización según se explica en el ANEXO D.

- Revisión de los derechos de acceso de los usuarios.

La política de seguridad es que el área de seguridad de la información debe realizar revisiones periódicas de los niveles de acceso otorgadas a los diferentes usuarios, tomado en cuenta los siguientes aspectos:

- ✓ Las revisiones de niveles de acceso se deberán realizar al menos una vez por semestre o en caso de ingreso, modificación o cancelación de un usuario.
- ✓ Los accesos a información crítica como administradores debe ser revisados cada trimestre.
- ✓ Los usuarios con privilegios especiales y los usuarios asignados al área de tecnologías deberán ser auditados constantemente, en especial si cuentan con derecho de acceso y manipulación total.

- Retirada o adaptación de los derechos de acceso.

Cuando un funcionario finalice su contrato o decida finalizar sus funciones dentro de la universidad, la política de seguridad manifiesta que se debe retirar todos los derechos de acceso a los sistemas, bases de datos y servidores para resguardar la información.

Para que esta política se cumpla, el jefe de cada departamento es el responsable de notificar al área de seguridad de la información, del cese de funciones de los usuarios para que la persona encargada de creación y eliminación de cuentas de usuario, elimine al usuario y los privilegios asignados.

- Responsabilidad del usuario

- Uso de información confidencial para la autenticación.

La política de seguridad es que los usuarios tengan claras las buenas prácticas de seguridad de la información, para mantener segura la información de la universidad. Para el cumplimiento de esta política los usuarios deben acoplarse a los siguientes lineamientos:

- ✓ La clave de ingreso a los sistemas de información, bases de datos y servidores deben ser estrictamente confidenciales e instransferibles.

- ✓ El usuario, por seguridad o en caso de sospecha de acceso no permitido por otra persona, debe cambiar periódicamente las claves de acceso.
- ✓ La contraseña de acceso de usuario debe ser compleja pero a la vez fácil de recordar, no deben contener una secuencia consecutiva de caracteres, además de no mantener relación con el nombre, teléfono o fecha de nacimiento del usuario, ya que pueden ser fáciles de obtener.
- ✓ No se debe mantener la clave provisionalmente otorgada.
- ✓ De existir alguna anomalía como perdida de clave, hurto de información o indicios de acceso a la cuenta de usuario sin autorización, se notificará de inmediato al área de seguridad de la información.

 Control de acceso a sistemas y aplicaciones

- Restricciones de acceso a la información.

La política de seguridad es restringir el acceso a los sistemas de la información a cada usuario, tanto a externos como a usuarios de la DITIC. Para el cumplimento de esta política se debe tener en cuenta los siguientes lineamientos:

- ✓ Cada sistema de información debe tener una página de *login*, en donde el usuario pueda autentificarse con un nombre de usuario y contraseña.
- ✓ Los usuarios deben saber información limitada de los sistemas, únicamente para el cumplimiento de sus funciones.
- ✓ Cada sistema debe permitir el acceso a la información autorizada y requerida, es decir se debe controlar los permisos de lectura, escritura y ejecución.
- ✓ Se debe realizar auditorías internas y externas, de ser necesario sobre el acceso y manipulación de la información.
- ✓ No permitir el acceso a la información de forma directa, únicamente a través de los sistemas de información.

- Procedimientos seguros de inicio de sesión.

En cuanto al inicio de sesión seguro, la política de seguridad se aplica a todas los sistemas desarrollados por la universidad, así como, a las aplicaciones de acceso de información, las mismas que deben tener una pantalla de acceso seguro de *log-on*, para asegurar que solamente personal autorizado tenga acceso.

Para el cumplimiento de esta política como se ha tratado en políticas anteriores, cada funcionario debe tener asignado un usuario y contraseña para acceso al sistema de información y por ende a bases de datos.

- Gestión de contraseñas de usuario.

Para la gestión de contraseñas, la política de seguridad es que la contraseña de acceso a los sistemas de información de cada usuario, debe tener un nivel de complejidad alto que dificulte obtenerla.

Para el cumplimiento de esta política, la universidad debe establecer la complejidad de las contraseñas, por ejemplo la contraseña debe constar de 16 caracteres entre letras, números y caracteres especiales, o usar un software administrador de contraseñas como *keePass*, que es un software portable que ayuda a la generación de contraseñas.

- Uso de herramientas de administración de sistemas.

En lo que tiene que ver con el uso de herramientas de administración, la política de seguridad es que los controles dentro de las aplicaciones deben estar restringidos, únicamente para los administradores de las aplicaciones se debe crear perfiles con acceso total, para evitar el acceso y modifican de información.

Para el cumplimiento de esta política se debe crear perfiles de usuario para cada uno de los funcionarios, dependiendo del nivel de acceso asignado. Únicamente los administradores de los sistemas de información pueden acceder a realizar modificaciones como parametrización o anulación de alguna transacción.

- Control de acceso al código fuente de los programas.

Restringir el ingreso al código fuente de las aplicaciones a usuarios externos y no autorizados de participar en el proyecto o desarrollo, para evitar la usurpación o cambio de código fuente.

Para el cumplimiento de esta política, cuando el analista, diseñador o programador abandone su puesto de trabajo ya sea por largo o corto tiempo, su máquina debe permanecer suspendida o apagada y con clave de acceso a la misma, y la clave no debe ser la misma que el nombre de usuario.

4.2.7. Cifrado

El objetivo de este dominio es el uso de sistemas y técnicas criptográficas para la protección de la información, en base a un análisis de riesgo efectuado previamente, con el fin de asegurar una adecuada protección. Las políticas planteadas en este dominio se basan en los controles publicados en el Portal ISO "Cifrado" [21].


Controles criptográficos

- Política de uso de controles criptográficos.

Definir el uso de controles criptográficos para asegurar la confidencialidad de la información y el correcto uso de la misma. Para el cumplimiento de esa política debemos tomar en cuenta los siguientes lineamientos:

- ✓ Los controles criptográficos se utilizarán para la protección de claves de acceso a servidores, base de datos y sistemas de información de ser necesario.
- ✓ Los controles criptográficos se utilizaran, para la trasmisión información confidencial mediante el uso de redes de datos desde la universidad.
- ✓ De la misma manera que se desarrollan procedimientos de encriptación, se debe desarrollar procedimientos de desencriptación.
- ✓ El área de seguridad de la información es la encargada de la implementación de controles criptográficos.
- ✓ El área de seguridad de la información deberá escoger el mejor algoritmo de encriptación y tamaño de claves.

Cifrado	Algoritmo	Longitud Clave
Asimétrico	RSA	2048 bits 1024 bits
	DSA	2048 bits 1024 bits
	ECDSA	210 bits
	SHA-1	256 bits
Simétrico	AES	128/192/256 bits
	3DES	128 bits
	IDEA	128 bits
	RC4	128 bits
	RC2	128 bits

Tabla Nº 10.- Algoritmos de encriptación

Elaborada por: Elizabeth Torres

El encargado del área de seguridad de la información deberá estar atento a las nuevas actualizaciones de los algoritmos para utilizar el más robusto y proteger la información.

- Gestión de claves.

La política de seguridad es gestionar el ciclo de vida de las claves criptográficas, dependiendo del algoritmo escogido en el control anterior.

Para el cumplimiento de esta política es necesario que la persona encargada de seguridad de la información establezca un tiempo prudente para el cambio de claves, en caso de utilizarlas dentro de la universidad. Además de establecer procedimientos para la creación, modificación, cambio y administración de claves.

4.2.8. La seguridad física y ambiental

El objetivo de este dominio es minimizar los riesgos de daños en la información y las operaciones de la organización, por desastres naturales o por falta de control en la seguridad física ante desastres ambientales. Además, de establecer los perímetros de seguridad de las áreas de procesamiento de información. Las políticas de seguridad planteadas en este dominio se basan en los controles establecidos y publicados en el Portal ISO "La seguridad física y ambiental" [22].

- Áreas seguras

  - Perímetro de seguridad física.

En lo que respecta a perímetros de seguridad, la política de seguridad debe restringir el acceso no autorizado a recursos tecnológicos que procesen información de la universidad, para preservar la confidencialidad de la información.

Para el cumplimiento de esta política los funcionarios deben cuidar los componentes tecnológicos, mantenerlos limpios, en buen estado, así como un registro de cada cambio que

se realice en la infraestructura física la misma que debe ser previamente analizada y debe enfocarse en proteger la información.

La UTA cuenta con áreas de procesamiento de información, protegida por control de acceso mediante biométrico, únicamente personal autorizado puede ingresas las áreas restringidas.

Dependiendo de la criticidad de la información que se maneje dentro de cada área de procesamiento de información, se deben establecer límites o perímetros de acceso. Las puertas del edificio donde se encuentra el área de procesamiento de información deben estar protegidas, las paredes deben ser sólidas, dentro y fuera de edificio debe estar vigilada por cámaras y alarmas sonoras.
Controlar el acceso a personal externo en la recepción, con una solicitud de identificación del personal externo. Las áreas que deben estar controladas son oficinas del departamento de sistemas, bodegas, oficinas de sistemas de cada carrera.

- Controles físicos de entrada.

La política de seguridad es que se deben establecer controles de acceso físico para poder acceder a las áreas de procesamiento de información.

Para el cumplimiento de esta política se debe inspeccionar al personal que ingresan a las áreas protegidas y llevar un registro de visitas con numero de cedula, nombre, hora de entrada, hora de salida.

Utilizar controles de autentificación como biométricos, tarjetas magnéticas, credenciales que siempre estén visibles, para limitar el acceso a información clasificada como confidencial o grado de criticidad media o alta. Se debe realizar periódicamente una revisión y actualización de los derechos de acceso a áreas protegidas.

- Seguridad de oficinas, despachos y recursos.

Mantener protegidas las oficinas, despachos y recursos donde se encuentren recursos tecnológicos y que procesen información, como prioridad las oficinas o departamentos de sistemas de cada facultad, donde se encuentran los servidores y cableado estructurado de la red de datos.

Para el cumplimiento de esta política se tomará en cuenta las siguientes medidas:

- ✓ Las oficinas de procesamiento de información deben ser discretas, y no deben ser fáciles de identificar.
- ✓ Se debe restringir el acceso a personal no autorizado a las instalaciones u oficinas que procesen información.
- ✓ Mantener seguras las ventanas y puertas de las oficinas de procesamiento de información, es decir mantener cerradas a menos que sea estrictamente necesario abrirlas. Dentro de estas oficinas deben estar los dispositivos como impresoras, plotters, fax, copiadoras, multifunciones.
- ✓ Separar las oficinas de procesamiento de información de la universidad y las administradas por terceros.
- ✓ Almacenar los respaldos de información en equipos seguros, distantes y en áreas protegidas. Evitar el acceso a información de contacto, de personal interno.

- Protección contra las amenazas externas y ambientales.

En lo que se refiere a protección contra amenazas, la política de seguridad es proteger la infraestructura contra desastres naturales como terremotos, inundaciones, fuego o desastres causados por el ser humano.

Para el cumplimiento de esta política las oficinas o áreas de procesamiento de información deben ubicarse en un lugar lejos de peligros como amenazas al fuego, escapes de agua en el techo o piso. Además de cumplir con los siguientes lineamientos.

- ✓ Las áreas de procesamiento de información deben mantenerse alejadas de materiales inflamables, combustibles, papelería o suministros de oficina.
- ✓ Los equipos de respaldo o reemplazo, servidores de contingencia deben estar ubicados en un área de procesamiento diferente a la de producción o ejecución.
- ✓ Proporcionar equipos anti-incendios y mantener actualizado y activo el plan de contingencia, para poder recuperar el área de procesamiento de información en el menor tiempo, ante un desastre.

- El trabajo en áreas seguras.

La política de seguridad es fortalecer la seguridad en el desarrollo de actividades y trabajo en las diversas áreas de la Universidad, para evitar causar algún desastre.

Para el cumplimiento de esta política se deben tomar en cuenta los siguientes lineamientos, que se aplican a personal interno y externo.

- ✓ Únicamente el personal que cumpla labores en áreas protegidas, deben conocer de su existencia.
- ✓ Los trabajos de remodelación o reconstrucción se lo debe realizar por personal interno, caso contrario debe ser supervisado por personal responsable del área dentro de la Universidad.
- ✓ El acceso de personal externo debe ser limitado, previamente autorizado y documentado.
- ✓ No permitir el acceso de equipos móviles como teléfonos, cámaras, dispositivos que registre información a menos que lo autorice el encargado del área de seguridad de la información.

- ✓ No permitir el ingreso de alimentos o bebidas al área de procesamiento de información.

- Áreas de acceso público, carga y descarga.

Para este control la política de seguridad es crear un área de carga y descarga para recepción de materiales o recursos tecnológicos que adquiera la Universidad, para evitar el acceso no autorizado a áreas restringidas.

Para el cumplimiento de esta política se debe tomar en cuenta los siguientes lineamientos.

- ✓ Las áreas de carga y descarga deben estar alejadas del área de procesamiento de información.
- ✓ El personal que entrega los suministros no podrán acceder a áreas restringidas de la universidad o de la facultad, únicamente tendrán acceso al área de carga o descarga.
- ✓ Proteger las puertas de acceso internas, cuando se realice una recepción de suministros o equipamiento.
- ✓ Revisar los suministros recibidos, para descartar peligros potenciales antes de trasladar al lugar de destino o antes de ubicarlos en el área asignada para su utilización.
- ✓ Registrar los suministros recibidos, que concuerde con los suministros pedidos por la universidad que conste con todas las características detalladas en el proyecto de adquisición.

- Seguridad de los equipos

- Emplazamiento y protección de equipos.

Para este control la política de seguridad es ubicar los equipos en un lugar seguro donde no estén expuestos a diversas amenazas físicas y ambientales para proteger la información.

Para el cumplimiento de esta política se debe tomar en cuenta que los equipos de procesamiento de información no se los debe instalar en lugares de libre acceso, adecuar áreas de procesamiento de información donde se encuentren los servidores, las mismas que tiene que estar permanentemente vigiladas y supervisadas. Además de ubicarlas en un lugar que no sea reconocido fácilmente, deben estar ocultas.

Únicamente el personal autorizado debe tener acceso a estas áreas, las mismas que serán examinadas semestralmente para evaluar los permisos de acceso asignados a cada uno y de ser necesario modificarlo.

- Instalaciones de suministro.

Para este control la política de seguridad es que las instalaciones donde se encuentran los equipos tecnológicos deberán estar protegidos y ser tolerantes a fallas eléctricas, para evitar pérdida de información, equipos tecnológicos y de comunicación.

Para el cumplimiento de esta política es necesario que el suministro de energía se adapte a los requerimientos de los equipos, tener varias tomas de energía con la finalidad de que si un punto de suministro de energía falla poder utilizar los otros puntos. En caso de cortes de energía mantener conectados los equipos a UPS que permitan tener el tiempo suficiente para apagar correctamente los equipos especialmente los servidores de bases de datos, aplicaciones y de red.

Dependiendo del nivel de criticidad de información que maneje cada departamento y la cantidad de equipos a proteger se deben adquirir los equipos UPS, se recomienda que por el nivel de información que se maneja se adquiera equipos como se detallan a continuación:

Departamento	UPS
Sistemas	30 minutos
Financiero	10 minutos
Secretarias	10 minutos
Direcciones de carrera	10 minutos

Tabla Nº 11.- UPS según departamento

Elaborada por: Elizabeth Torres

Además deberá existir un sistema de iluminación de emergencia, y realizar revisiones periódicas de los suministros de energía para evitar daños y asegurar su correcto funcionamiento.

- Seguridad del cableado.

En cuanto a seguridad de cableado, la política de seguridad es que el cableado de datos y eléctrico debe ser protegido contra daños ya sean provocados, e interrupciones para evitar desastres.

Para el cumplimiento de esta política el cableado de datos y eléctrico debe estar protegido por canaletas, tuberías o subterráneo para evitar interrupciones no autorizadas, evitar que el cableado este a la vista del público.

El cableado eléctrico y de datos debe estar separado para evitar pérdidas de paquetes de datos e interferencias, además los cables de datos deben estar identificados por etiquetas así como los puntos de red en el patch panel para facilitar la manipulación y evitar errores. Documentar el mapa de red de cada departamento o facultad y mantenerlo actualizado.

Para los servidores de bases de datos, repositorios o procesadores de información se debe utilizar cajas con seguridad para los puntos de inspección, de ser posible utilizar fibra óptica

y tubos blindados. Para el acceso del personal a revisiones a los puntos de conexión y empalmes debe ser controlado y registrado.

Se debe realizar revisiones trimestrales de los dispositivos conectados a la red de datos para evitar dispositivos que representen una amenaza a la seguridad de la información. La principal concentración del cableado y por ende la más restringida debe ser el data center de la universidad, y los departamentos de sistemas de cada facultad seguido de las bibliotecas y direcciones de carrera.

- Mantenimiento de los equipos.

Para este control la política de seguridad es brindar mantenimiento continuo a los equipos que pertenecen a la universidad en especial a los que procesen información, para asegurar la disponibilidad de los mismos.

Para el cumplimiento de esta política se deben tomar en cuenta las recomendaciones del fabricante de los equipos, solamente el personal de sistemas de cada facultad están autorizados a dar mantenimiento a los equipos y luego de realizar el mantenimiento se colocara sellos de garantía.

Mantener una bitácora digital o manual, en la que se debe señalar los posibles daños o cambios de piezas y posibles fallas de cada uno de los equipos, al personal de sistemas se les prohíbe la divulgación o copia de la información almacenada en los equipos. El encargado del área de seguridad de la información en caso de tener contratado un seguro para los equipos debe observar los requerimientos impuestos por la empresa.

- Salida de activos fuera de las dependencias de la universidad.

En cuanto a la salida de activos fuera de la universidad, la política de seguridad es que los equipos portátiles o tecnológicos que tengan información de la institución no salgan de su sitio de trabajo, sin previa autorización.

Para el cumplimiento de esta política se debe tener en cuenta, que los equipos otorgados para realizar labores dentro de la universidad, deben permanecer en su sitio de trabajo y utilizarlos únicamente para labores relacionados con la misma.

De requerir su uso fuera de las oficinas debe ser bajo autorización del encargado del área de seguridad de la información, no descuidarlo mientras esta fuera, mantenerla siempre cerca y seguir las recomendaciones de fábrica para los equipos portátiles o tecnológicos.
Los equipos portátiles deben estar protegidas con claves de acceso y luego de un período de tiempo de inactividad obligar a autentificarse, la información que se almacene debe estar encriptada o almacenada en un lugar que no sea visible, cuando se requiera teletrabajo la conexión hacia los servidores debe ser atreves de VPN, y los datos a transferir deben estar encriptados.

- Seguridad de los equipos y activos fuera de las instalaciones.

La política de seguridad es proteger la información que se encuentre en los equipos que procesen información fuera de la universidad, para asegurar la disponibilidad, confidencialidad de la información.

Para el cumplimento de esta política se debe asegurar el traslado de los equipos, tomando en cuenta las recomendaciones de fábrica, como se trató en la política anterior los datos que se manejen dentro de estos dispositivos deben estar encriptados, y al realizar la conexión a la red de datos la trasferencia debe estar encriptada.

- Reutilización o retirada segura de dispositivos de almacenamiento.

En cuanto a reutilización o retirada de dispositivos de almacenamiento, la política de seguridad es revisar que los dispositivos conectados a los equipos se retiren sin contener información sensible o software licenciado.

Para el cumplimiento de esta política es necesario que cuando se retire un dispositivo de almacenamiento de los equipos, se verifique que no contenga información sensible o datos de licencias de software. El encargado del área de sistemas de cada facultad debe realizar esta revisión, únicamente personal autorizado debe poder conectar dispositivos de almacenamiento en equipos q contengan información sensible.

- Equipo informático de usuario desatendido.

La política de seguridad es que el administrador de redes y sistemas de cada facultad realice revisiones periódicas de los equipos que no están en constante uso, en especial de los equipos que procesen información.

Para el cumplimiento de esta política es necesario que el administrador de redes y sistemas verifique que estos equipos estén protegidos con contraseñas, que se encuentren en un lugar seguro donde no exista humedad o filtraciones de agua, y que todas las conexiones de datos y eléctricas sean seguras.

Además los datos que se encuentren en estos equipos debe estar encriptados, deben contar con un antivirus actualizado, permanentemente se le debe realizar mantenimiento y limpieza física y de archivos temporales.

- Política de puesto de trabajo despejado y bloqueo de pantalla.

Para puestos de trabajo despejados y bloqueos de pantalla, la política de seguridad es mantener la información protegida, cuando el funcionario se aleja de su puesto de trabajo por un corto o largo tiempo, bloquear la pantalla en un lapso de tiempo prudente de inactividad.

Para el cumplimiento de esta política es necesario que los equipos requieran autentificación luego de un tiempo de desuso o inactividad, el tiempo recomendado es de 5 minutos. Además, el funcionario debe tener presente cuando salga de su puesto de trabajo tiene que cerrar todas las actividades que esté realizando en los sistemas de información, bases de datos y administración de servidores o redes.

En los equipos de procesamiento de información únicamente se conectarán medios de almacenamiento extraíbles que pertenezcan a la universidad y con previa revisión y autorización del encardado del área de procesamiento, para evitar filtro de información en medios extraíbles.

4.2.9. Seguridad en la operativa

El objetivo de este dominio es, controlar la existencia de documentación de los procedimientos de operaciones, planes de contingencia además de la mejora y mantenimiento continuo de los mismos, para el acceso no autorizado se debe definir y documentar controles, protección contra software malicioso y documentación para resguardar la seguridad de la base de datos y la restauración de copias de seguridad. Las políticas de seguridad se basan en los controles publicados en el Portal ISO "Seguridad en la operativa" [23].

- Responsabilidades y procedimientos de operación

  - Documentación de procedimientos de operación.

Para este control, la política de seguridad es la creación y documentación de los procedimientos operativos de los diversos sistemas de información que utiliza la UTA.

Para el cumplimiento de esta política se debe documentar los procedimientos operativos, manejo de errores generales y restricciones de uso de todos los sistemas de la universidad. Además, para realizar una modificación debe ser previamente autorizada por el encargado del área de seguridad de la información y luego se debe actualizar el documento.

Documentar los procedimientos de instalación, cambio o modificación de servicios, módulos o complementos de los sistemas, además de los procedimientos de reinicio de sistemas, para garantizar la calidad y confiabilidad de los servicios ya sea por procedimientos rutinarios o por fuerza mayor.

Documentar los procedimientos de mantenimiento, instalación y monitoreo de equipos y servidores en este caso documentar el resguardo de información, respaldos y uso de correos electrónicos. Además, se debe mantener una bitácora sobre la información del personal técnico en caso de errores y problemas operativos.

  - Gestión de cambios.

En cuanto a la gestión de cambios, la política de seguridad es que antes de realizar un cambio en el ambiente operativo, este debe ser evaluado y documentado por el encargado del área de seguridad de la información en conjunto con el personal de la DITIC.

Para el cumplimiento de esta política, se debe evaluar las posibles implicaciones, estos cambios deben ser requeridos por los usuarios de la información, evaluados y aprobados por el director del departamento o por la persona que este encargado del área. Se debe mantener una bitácora de los cambios realizados en los diversos sistemas y antes de realizar un cambio sacar una copia de respaldo.

Tiene que ser documentado los registros de cambios en la infraestructura, posibles implicaciones, aprobación y planificación del cambio, procedimiento para reversar el cambio, matriz de problemas presentados durante el cambio con sus respectivas soluciones.

- Gestión de capacidades.

En cuanto a la gestión de capacidades, la política de seguridad es monitorear el rendimiento de los sistemas de información para optimizar los recursos dependiendo de la capacidad de información y requerimientos a futuro.

Para el cumplimiento de esta política es necesario que el encargado del área de seguridad de la información monitoree el rendimiento de los sistemas que maneja la universidad, para realizar cambios en tecnologías o metodologías, y garantizar el rendimiento adecuado de los sistemas tomando en cuenta las influencias futuras.

Analizar las mejores metodologías y tecnologías para implementar en los sistemas de información y mejorar sus tiempos de respuestas y manipulación de datos.

- Separación de entornos de desarrollo, prueba y producción.

Para este control la política de seguridad es crear entornos para las principales fases del ciclo de vida de un proyecto, desarrollo, pruebas y producción de preferencia deben separarse físicamente, cuando se debe trasladar un sistema o servicio entre entornos, este traslado debe ser documentado.

Para el cumplimiento de esta política es necesario que cada ambiente se desarrolle en servidores, fases, tipos de sistemas y áreas físicas diferentes, para evitar que el área de desarrollo y código fuente tenga libre acceso.

Mantener documentado los nombres del personal que colabora con el desarrollo de los proyectos, con los cargos y responsabilidades, los mismos que deben mantenerse en sus funciones y no tener acceso a las demás áreas a menos que sea requerida y sea autorizada por el área de seguridad de la información.

- Protección contra código malicioso

  - Controles contra el código malicioso.

La política de seguridad es construir controles técnicos o no técnicos para proteger la información e infraestructura tecnológica contra virus, malware y concienciar a los usuarios sobre la sensibilidad de la información.

Para el cumplimiento de esta política es necesario que no se instalen o utilicen software que no sea autorizado por el área de seguridad de la información, en cada uno de los laboratorios de la universidad deberán estar instalados únicamente los programas necesarios para el aprendizaje de los estudiantes. Se recomienda mantener congeladas las maquinas, es decir proteger los ordenadores de trabajo de cualquier cambio o problema grave y poder restaurarlos si fuera necesario. Se recomienda utilizar Deep Freezer que permite restaurar las configuraciones de la maquina al reiniciarla.

Todo el software que se utilice por los funcionarios de la universidad debe estar dentro de las leyes vigentes de la Universidad, además de inculcar la cultura informática a los funcionarios de las implicaciones que podrían causar la instalación de software ilegal.

Mantener un registro del software instalado en los equipos, el mantenimiento se lo realizara únicamente al software autorizado por el departamento de sistemas de cada facultad, además de realizar revisiones periódicas del software instalado.

La universidad cuenta con la consola de *Kaspersky*, un antivirus que permite la gestión de todas las maquinas en red para evitar malware o virus que pueden atacar a los equipos, se debe administrar las actualizaciones automáticas, permite monitorear si es potencialmente peligrosa una máquina o si se encuentra un programa peligroso. Los sistemas operativos y programas siempre deben estar actualizados.

El departamento de sistemas es el encargado de realizar el monitoreo y actualización de los programas y los funcionarios deben reportar a este departamento sobre cualquier problema de virus o software malicioso.

- Copia de seguridad

  - Copias de seguridad de la información.

En cuanto a copias de seguridad, la política de seguridad es comprobar que las copias de seguridad funcionen correctamente, y que los respaldos se realicen de acuerdo a los tiempos y días acordados.
Para el cumplimiento de esta política es necesario que se asigne un responsable para que realice las copias de seguridad, pruebas y restauraciones de los sistemas de información y bases de datos.

Los respaldos de información deben estar en un lugar seguro, con controles de acceso necesarios y en un área física adecuada, se debe tomar en cuenta los siguientes lineamientos:

- ✓ Documentar el listado de bases de datos y sistemas a respaldar con su frecuencia.

- ✓ Realizar un manual de procedimientos para respaldos donde se definirá el tipo de respaldo que se requiere para cada sistema.
- ✓ Los respaldos se los sacara en discos o dispositivos, que se encuentren en áreas en las que sería menos probable la incidencia de algún desastre natural, los mismos que deben ser probados periódicamente.
- ✓ Se debe documentar los procedimientos a seguir para la restauración de los respaldos de información, y dependiendo del nivel de criticidad o confidencialidad de información que contenga debe ser encriptada.
- ✓ En los casos de sistemas de información críticos el respaldo será total, de aplicación y base de datos, y determinar por escrito cuanto tiempo se retendrá la información en los medios de almacenamiento.
- ✓ En caso de utilizar herramientas que realicen respaldos automáticos, la herramienta debe estar probada en todas sus fases y ser de total confianza.

- Registro de actividad y supervisión

  - Registro y gestión de eventos de actividad.

Para el registro y control de eventos, la política de seguridad es crear campos de auditoria para controlar y revisar periódicamente las actividades que cada usuario realiza, además de añadir excepciones para evitar errores y fallas en los sistemas.

Para el cumplimento de esta política es necesario crear *triggers* de auditoria mediante la base de datos, y creación de tablas de auditoria las mismos que se actualizarán cuando un usuario cree, elimine o edite un registro en la base de datos.

También en los sistemas de información desarrollados por la universidad deben contener excepciones para el control de fallas y errores que se pueden producir en los sistemas, para proteger la integridad de la información.

- Protección de los registros de información.

Para este control la política de seguridad es que cada usuario que ingrese a los sistemas de información de la universidad tenga asignado un rol dependiendo de las funciones que vaya a realizar para proteger la información de manipulaciones no permitidas.

Para el cumplimiento de esta política es necesario que cada uno de los usuarios tenga definido las actividades y permisos de manipulación de datos, para la creación y asignación de roles, además de que los sistemas de información deben ser multiusuarios, y flexible a cambios de roles.

- Registros de actividad del administrador y operador del sistema.

En cuanto a las actividades del administrado, la política de seguridad es registrar cada una de las actividades que realiza el administrador y operadores de los sistemas de información de cada una de las facultades.

Para el cumplimiento de esta política es necesario que los funcionarios de los departamentos de sistemas de cada una de las facultades o departamentos lleven un registro de sus actividades, se debe registrar la hora, el tipo y acción realizada, los usuarios involucrados, y todas las tareas o acciones secundarios para llevar acabo la actividad, para cumplir con esta política es necesario en las bases de datos se incrementen tablas o procedimientos de auditoria.

- Sincronización de relojes.

Para este control la política de seguridad es sincronizar los relojes de todos los sistemas de procesamiento de información, así como los de bases de datos para tener un registro real de las transacciones realizadas.

Para el cumplimiento de esta política es necesario tener un reloj fuente con la hora exacta según la zona horaria para la región continental de Ecuador (GMT-5), el que no se debe cambiar por ningún motivo, esto permitirá que las transacciones realizadas en los sistemas de información y bases de datos se realicen a la hora exacta.

- Control del software en explotación

  - Instalación del software en sistemas en producción.

La política de seguridad es que se debe planificar los cambios en los sistemas de información y realizar pruebas con el fin de asegurar el correcto funcionamiento.

Para el cumplimiento de esta política es necesario que todos los funcionarios involucrados hayan sido notificados con anterioridad del cambio el mismo, y asegurar que el cambio no afecte las funcionalidades de los sistemas de información.

- Gestión de vulnerabilidades técnicas

  - Gestión de las vulnerabilidades técnicas.

Mantener actualizado el inventario de los equipos físicos y de software como fecha de compra, vida útil, versión, actualizaciones o *service packs* instalados, para evitar daños en los equipos por software instalado o por tiempo de vida útil de los equipos.

Para el cumplimiento de esta política es necesario asignar un responsable para el monitoreo y exploración de las vulnerabilidades, el mismo que deberá realizar una planificación en línea de tiempo de las vulnerabilidades existentes.

Cuando se identifique la vulnerabilidad se debe realizar un análisis de los riesgos y acciones a realizarse para mitigar la vulnerabilidad, dependiendo de la criticidad del riesgo primero se

deberá probar y evaluar antes de ser instaladas en el ambiente de producción, luego se realizaran las acciones necesarias como actualizaciones, parches o demás configuraciones técnicas.

En caso de que los fabricantes no cuenten con el parche o la actualización se debe desconectar los servicios, agregar controles de acceso, incrementar el monitoreo, mantener el registro de auditoria de todos los procedimientos, tratar primero los sistemas de mayor criticidad y la gestión de la vulnerabilidad debe ser monitoreada y evaluada.

- Restricciones en la instalación de software.

La política de seguridad es controlar las aplicaciones y software instalado en las computadoras de cada uno de los funcionarios de la universidad.

Para el cumplimiento de esta política es necesario la revisión y mantenimiento periódico de los equipos de la universidad, este procedimiento lo llevará a cabo el encargado del área de sistemas de cada facultad, el mismo que debe cerciorarse de que únicamente se encuentre instalado software autorizado y de uso específico para realizar las actividades encomendadas, para evitar el filtro de información. Además, evitar la instalación de software inapropiado como juegos, *hacking*, envió automático de correos con información de la universidad, entre otros.

- Consideraciones de auditorías de los sistemas de información

- Controles de auditoría de los sistemas de información.

Para este control la política de seguridad es realizar auditorías internas y externas periódicamente para verificar el correcto funcionamiento de los sistemas de información.

Para el cumplimiento de esta política es necesario que los procedimientos de auditoria deben realizarse en el periodo acordado, los registros que deben constar dentro de la auditoria son:

- ✓ Nombre o ID de usuario.
- ✓ Hora y fecha de ingreso y salida.
- ✓ Hora y fecha de actualización
- ✓ Dirección IP y nombre del equipo de donde se inició sesión.
- ✓ Mantener un registro de intentos fallidos y permitidos.
- ✓ Cambios de configuración de los perfiles de usuario
- ✓ Bitácora y monitoreo de los accesos a utilidades, aplicaciones y oficinas de procesamiento de información.
- ✓ Control de activación y desactivación de sistemas de protección como por ejemplo el anti-virus.

El encargado del departamento de sistemas de cada facultad o administrador de sistemas, no deberá tener permisos para borrar o eliminar los controles de auditoria, además de que las actividades que el realice deberán ser auditadas.

4.2.10. Seguridad en las telecomunicaciones

El objetivo del presente dominio es asegurar la protección de la información que se comunica por redes telemáticas y la protección de la infraestructura de soporte, la gestión de seguridades en las telecomunicaciones considera el flujo de datos, implicaciones legales internas y externas. El intercambio de información entre instituciones y redes públicas debe ser confidencial. Las políticas de seguridad planteadas en el presente dominio procuran cumplir con los objetivos publicados en el Portal ISO "Seguridad en las telecomunicaciones" [24].

- Gestión de la seguridad en las redes

  - Controles de red.

En relación al control de red la política de seguridad es administrar y monitorear las redes continuamente, manteniendo la seguridad y garantizando que la información transmitida este segura y libre de acceso no autorizado.

Para el cumplimiento de esta política el área de redes será la encargada de administrar y monitorear las redes continuamente tomando en cuenta los siguientes lineamientos:

- ✓ El área de administración de red debe establecer responsabilidades de tareas como administración y monitoreo de redes, incluyendo equipos de comunicación, enrutadores, *switchs* y canales de comunicación.
- ✓ Agregar controles extras para asegurar la confidencialidad de la información transmitida por internet o redes inalámbricas. Se puede utilizar Redes Virtuales Privadas (VPN) o encriptación sobre las redes inalámbricas.
- ✓ Debe existir un registro de acceso a la red para controlar la actividad realizada y si existe alguna anormalidad.
- ✓ Para los equipos de conectividad hay que cambiar las configuraciones por defecto. Además, se debe cerrar la sesión durante 30 segundos de inactividad, guardar registros de auditoria, sacar respaldos de configuración de los *switchs* al menos una vez al mes.
- ✓ Para los equipos de interconexión inalámbrica usar puntos de acceso inalámbrico (Access Point), deshabilitar el *broadcast*, debe ser de acceso libre sin contraseña.

- Mecanismos de seguridad asociados a servicios en red.

En cuanto a mecanismos de seguridad asociados a servicios en red, la política de seguridad es que cada servicio que se desee implementar externo o interno, debe incluir características de seguridad que asegure la integridad de la información.

Para el cumplimiento de esta política el director de sistemas debe monitorear el rendimiento y la capacidad operativa del proveedor de servicios si este fuera externo, para verificar la concordancia de los requerimientos de la universidad como el nivel de seguridad. Los servicios de red deben incluir VPNs, soluciones de seguridad firewalls, sistema de prevención de intrusos implementadas por terceros o por la universidad.

Los servicios de red deben tener controles de autentificación, acceso, cifrado y requerimientos para una conexión segura establecida por la universidad.

- Segregación de redes.

Para segregación de redes, la política de seguridad es dividir la red de datos en dominios lógicos y mantener los segmentos de red separados.

Para el cumplimiento de esta política se debe documentar los segmentos de red utilizados para cada facultad y departamento con perímetros de seguridad, además de complementar con la instalación de *gateways* con funcionalidades de *firewalls* o redes virtuales privadas y la aplicación de políticas de control de acceso.

Las redes pueden se segregadas por IP *switching* y enrutamiento controlando el tráfico entre los segmentos y configuraciones de enrutamiento. Además de establecer requerimientos de seguridad del dominio y segmentos de red, definir que grupos integran los segmentos de red, segmentar los grupos expuestos a peligros externos.

La universidad segrega las redes mediante VLANs para facultades, las mismas que se divide en VLANs para laboratorios que separa las redes de los diferentes laboratorios y departamentos administrativos.

- Intercambio de información con partes externas

  - Políticas y procedimientos de intercambio de información.

Para el intercambio de información, la política de seguridad es autorizar y revisar todo tipo de información que se transfiera a organismos externos y por cualquier medio de comunicación.

Para el cumplimiento de esta política es necesario tomar en cuenta el medio por el cual se realizara la transmisión de la información, si es manual se debe entregar personalmente al destinatario en un sobre sellado y la entrega debe ser registrada.

Si el intercambio es vía correo electrónico, se debe realizar por el correo institucional y la información enviada debe contener una advertencia en cuanto al uso y autorizaciones de uso de la información, quedando la responsabilidad de cuidado y resguardo de la información sobre el receptor. Además, la información debe ser encriptado durante la trasmisión para protegerla. Si el intercambio es por otra medio, se debe cumplir la política de control de acceso y seguridad de red, la transmisión de información sensible vía teléfono queda prohibida.

Para el intercambio de información por interoperación entre sistemas se debe realizar decretos externos este documento aprueba y define la prestación de servicios mutuos, especifica la organización necesaria para su cumplimiento, las obligaciones, costos, incumplimientos y responsabilidades, es un documento público que aprueba el convenio de cooperación o de interoperabilidad debe ser autorizado y firmado por la máxima autoridad.

- Acuerdos de intercambio.

Para acuerdos de intercambio, la política de seguridad es asegurar la información a transferir a organizaciones externas, si es necesario la información debe ser encriptado para su transmisión.

Para el cumplimiento de esta política es necesario que la información a trasferir sea previamente autorizada y que únicamente se trasfiera lo necesario. Cuando la transferencia es vía electrónica debe ser encriptado y establecer acuerdos de confidencialidad de la información entre las organizaciones y la universidad, donde se considere que el responsable de cuidar y resguardar la información es la persona u organización que la reciba. Además este acuerdo debe ser firmado por las dos partes.

- Mensajería electrónica.

La política de seguridad, es la utilización del correo institucional para envió y recepción de información, para su protección se debe revisar periódicamente la información que se envía y se recibe en las cuentas de correo electrónico.

Para el cumplimiento de esta política es necesario que el encargado del área de sistemas monitoree la información que se maneja en las cuentas de correo y en la mensajería instantánea. Para los funcionarios está prohibido trasferir información por correo personal al menos que sea autorizado previamente por la autoridad máxima de la universidad.

- Acuerdos de confidencialidad y secreto.

Para este control, la política de seguridad es identificar, revisar y documentar regularmente los acuerdos de confidencialidad de la información que la universidad tiene para evitar su divulgación.

Para el cumplimiento de esta política es necesario que el director de la DITIC asigne la responsabilidad de revisar continuamente los acuerdos de confidencialidad a un funcionario del área de sistemas, el mismo que revisará e informara a la dirección los cambios que crea necesarios, los mismos que serán analizados y autorizados para realizar los cambios en los acuerdos.

4.2.11. Adquisición, desarrollo y mantenimiento de los sistemas de información

El presente dominio tiene por objetivo la adquisición, desarrollo y mantenimiento de los sistemas de información que la universidad maneja, incluir controles para la validación de datos y correcto funcionamiento durante la adquisición y desarrollo. Aplicar procedimientos de control durante todo el ciclo de vida de desarrollo de proyectos incluyendo la protección de información crítica y sensible. Las políticas planteadas en este dominio aplican a todos los sistemas de información ya sean desarrollos propios o de terceros, estas políticas se basan en los controles publicados en el Portal ISO "Adquisición, desarrollo y mantenimiento de los sistemas de información" [25].

- Requisitos de seguridad de los sistemas de información

  - Análisis y especificación de los requisitos de seguridad.

Para este control, la política de seguridad es analizar y especificar los requerimientos de seguridad de la información para las mejoras y nuevos sistemas de información.

Para el cumplimiento de esta política es necesario que en la etapa de análisis y diseño del sistema, se incluyan mecanismos de seguridad de la información, sin afectar el producto final y que cumpla con las necesidades del usuario. Es necesario realizar un análisis de riesgos previo al desarrollo e implementación para definir los requerimientos de seguridad y los procedimientos apropiados.

Es importante tomar en cuenta los riesgos envueltos, los costos económicos y el rendimiento implicados al aplicar las seguridades en las aplicaciones. Los costos económicos de implementación y mantenimiento son menores cuando las seguridades se las aplica desde la etapa de diseño.

- Seguridad de las comunicaciones en servicios accesibles por redes públicas.

En cuanto a seguridad de las comunicaciones en servicios accesibles por redes públicas, la política de seguridad es proteger la información que pasa atreves de las aplicaciones que utilizan redes públicas para transferirla.

Para el cumplimiento de esta política, es necesario que al momento de transferir la información esta sea encriptado para evitar el ingreso o cambio no autorizado, el encargado del área de seguridad de la información debe analizar a profundidad, los servicios que acceden a redes públicas y evaluar los riesgos y vulnerabilidades, establecer los procedimientos necesarios para proteger la información que interviene en el correcto funcionamiento de los servicios.

- Protección de las transacciones por redes telemáticas.

La política de seguridad es proteger la información de la transmisión o enrutamiento incorrecto y evitar la alteración duplicación o divulgación no autorizada.

Para el cumplimiento de esta política es necesario que se realice revisiones periódicas del funcionamiento y almacenamiento de la información que procesan los sistemas, para verificar si se está almacenado en el lugar correcto y evitar la alteración, divulgación y/o duplicación no autorizada.

- Seguridad de los procesos de desarrollo y soporte

  - Política de desarrollo seguro de software.

Para el desarrollo de software seguro, la política de seguridad es constituir y aplicar reglas para el desarrollo de sistemas para proteger la información y el código fuente de los sistemas.

Para el cumplimiento de esta política es necesario estandarizar el ciclo de desarrollo de los sistemas, dependiendo de la metodología de desarrollo definida por la universidad, además de estándares de seguridad y de calidad. Todos estos estándares deben estar documentados y autorizados por el director de la DITIC.

Los programadores o terceros que se incluyan al desarrollo del proyecto, no deben tener acceso a información de producción que contenga datos sensibles. Para desarrollo y pruebas se deben generar datos propios. Además se debe crear un ambiente amigable entre el grupo de desarrollo y proporcionar una área segura con todos los controles de seguridad establecidos en dominios anteriores.

  - Procedimientos de control de cambios en los sistemas.

En relación a procedimientos de control de cambios en los sistemas, la política de seguridad es mitigar los riesgos por cambios sobre el software ya sean estos planificados o requeridos.

Para el cumplimiento de esta política es necesario que todo cambio requerido sea por escrito el mismo que lo debe hacerse por personal calificado, en el caso de que el cambio requiera manipulación de datos, se debe tener la autorización e identificar los elementos a modificarse (software, bases de datos, hardware).

Llevar una bitácora sobre le personal y el nivel de acceso que tenga para realizar cambios en los sistemas de información. Revisar y actualización periódicamente la documentación de los estándares y mecanismos para mantener la integridad de los datos.

Todos los cambios se los debe desarrollar en el área de desarrollo, además antes de ser implementados deben ser probados y aprobados por el responsable de área de sistemas y el encargado de la seguridad de la información y de ser necesario un usuario del sistema.

Al realizar los cambios se debe garantizar que no se interrumpa el funcionamiento de los servicios en especial los que sustentan las operaciones del departamento; el departamento o personal debe ser comunicado con anterioridad sobre el cambio. Garantizar que el cambio o actualización se lo realice por el personal autorizado y capacitado.

- Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.

Para este control la política de seguridad es garantizar que los cambios realizados en los sistemas de información no tengan un impacto negativo en las operaciones y seguridad de los sistemas de información.

Para el cumplimiento de esta política es necesario monitorear y realizar pruebas para asegurar el correcto funcionamiento de los sistemas de información sometidos a actualizaciones o cambios, sin interrumpir el rendimiento de las funcionalidades del sistema raíz, el personal involucrado en dicha actualización debe ser notificada con anticipación.

- Restricciones a los cambios en los paquetes de software.

En cuanto a restricciones a los cambios en los paquetes de software, la política de seguridad es realizar modificaciones de los paquetes de software suministrados por terceros estrictamente los necesarios.

Para el cumplimiento de esta política es necesario que el encargado del área de sistemas de cada facultad o departamento evalúe las modificaciones a los paquetes que sean necesarios, sin afectar la integridad, confidencialidad y disponibilidad de la información. Las modificaciones a los paquetes debe ser previamente autorizado por el director de la DITIC.

- Uso de principios de ingeniería en protección de sistemas.

Para este control la política de seguridad es aplicar principios de seguridad en la ingeniería de sistemas las mismas que serán documentadas, y actualizadas permanentemente.

Para el cumplimiento de esta política es necesario que el director de la DITIC asigne un responsable para la investigación e implementación de los principios de seguridad en ingeniería de sistemas. Este responsable debe realizar un análisis previo la implementación de los sistemas de información.

- Seguridad en entornos de desarrollo.

Para los entornos de desarrollo la política de seguridad es proteger adecuadamente los entornos de desarrollo que cubre todo el ciclo de vida de desarrollo del sistema.
Para el cumplimiento de esta política es necesario crear un entorno adecuado para el desarrollo de sistemas, tomando en cuenta las políticas de control de acceso y seguridades físicas y ambientales para la protección de los equipos de desarrollo. En cuanto el personal crear un ambiente de trabajo confortable, en donde el personal se sienta grato.

- Externalización del desarrollo de software.

En cuanto a externalización del desarrollo de software la política de seguridad es monitorear y supervisar cada una de las actividades del desarrollo de sistemas que se realicen fuera de la universidad.

Para el cumplimiento de esta política es necesario asignar un responsable para el monitoreo de las actividades de desarrollo externalizadas, es necesario que los desarrolladores de los sistemas tengan claro que toda creación, innovación, producto u objeto creado dentro de la universidad será propiedad de la misma.

Además los productos o programas externalizados deberán ser entregados en el tiempo acordado, incluyendo manuales, descripción técnica y documentación.

- Pruebas de funcionalidad durante el desarrollo de los sistemas.

Para este control la política de seguridad es realizar pruebas de funcionalidad y en especial de seguridad, durante la etapa de desarrollo para evitar desperfectos en el producto final.

Para el cumplimiento de esta política es necesario elaborar una planificación de pruebas con usuarios reales, para evaluar el nivel de seguridad de los sistemas y de ser necesario cambiar los criterios o procedimientos empleados para proteger la información. Además documentar las pruebas realizadas, con la fecha de las pruebas y las observaciones realizadas por los usuarios que realicen las pruebas.

- Pruebas de aceptación.

En cuanto a pruebas de aceptación, la política de seguridad es elaborar un plan de pruebas y el ambiente en el que se realizara las pruebas para la aceptación de los nuevos sistemas o actualizaciones de versiones.

Para el cumplimiento de esta política es necesario que se asigne un responsable para la elaboración del plan de pruebas que debe ser aprobado por el director, él mismo que tiene que asignar pilotos y datos de acceso para el desarrollo de las pruebas. Estas pruebas deben arrojar incidencias, mejoras, detección de código malicioso y observaciones, las que deben constar en un acta de reuniones.

En caso de incluir incidencias o mejoras deberá existir una segunda prueba con los mismos pilotos y datos de acceso, y así sucesivamente hasta que el sistema sea aprobado en su totalidad y no exista ninguna observación.

- Datos de prueba

  - Protección de los datos utilizados en pruebas.

En cuanto a protección de los datos utilizados en pruebas, la política de seguridad es clasificar cuidadosamente los datos a utilizar para pruebas evitando que se utilicen datos sensibles.

Para el cumplimiento de esta política es necesario prohibir el uso de bases de datos operacionales en el ambiente de pruebas, de ser necesario utilizar herramientas para la generación de datos personalizados. Si se requiere utilizar los registros de las bases de datos operacionales se debe despersonalizar los datos antes de ser utilizada.

4.2.12. Relaciones con suministradores

El presente dominio pretende implementar y mantener el nivel de seguridad de la información, mediante los acuerdos de entrega de servicios de terceros, monitorear el cumplimiento de dichos acuerdos acorde con los estándares y manejos de cambios para satisfacer los requerimientos acordados de los servicios entregados. Las políticas de seguridad planteadas en este dominio se basan en los controles publicados en el Portal ISO "Relaciones con suministradores" [26].

- Seguridad de la información en las relaciones con suministradores

  - Política de seguridad de la información para suministradores.

La política de seguridad es establecer y documentar los requerimientos de seguridad de la información para mitigar los riesgos de acceso no autorizado por parte de proveedores y terceros.

Para el cumplimiento de esta política es necesario analizar los riesgos a la que está expuesta la información de accesos no autorizados por terceros, de acuerdo a dicho análisis establecer los requerimientos de seguridad en aprobación con el director y jefes de áreas de la DITIC, estos requerimientos deben ser documentados y actualizados permanentemente o cada que se requiera. Estos requerimientos de seguridad deben ser presentados y acordados por la universidad y los proveedores o terceros que tienen acceso a la información.

  - Tratamiento del riesgo dentro de acuerdos de suministradores.

Para el tratamiento de riesgos con suministradores, la política de seguridad es establecer y documentar los requerimientos de seguridad de la información para proveedores que tengan acceso a componentes de infraestructura de TI que dan soporte a la Información.

Para el cumplimiento de esta política es necesario cumplir con la política de seguridad de la información para suministradores, y establecer políticas de seguridad para las componentes de TI para dar mantenimiento a la información, revisar las configuraciones de fábrica de los componentes adquiridos para mantenimiento.

Solamente de ser necesario utilizar suministros externos para realizar mantenimiento, caso contrario utilizar herramientas pertenecientes a la universidad, para asegurar que la información no sea filtrada por terceros.

- Cadena de suministro en tecnologías de la información y comunicaciones.

Para suministros en cadena, la política de seguridad es establecer y documentar los requerimientos de seguridad de la información que se adquieren en cadena de los diferentes proveedores, para mitigar el riesgo de acceso no autorizado y el cumplimiento con las políticas anteriores de este control.

Para el cumplimiento de esta política es necesario que el encargado del área de seguridad de la información elabore un documento de procedimientos a seguir, considerando las seguridades necesarias para proteger la información, para la adquisición de suministros frecuentes a los proveedores.

- Gestión de la prestación de servicios por suministradores

- Supervisión y revisión de los servicios prestados por terceros.

Para este control, la política de seguridad es auditar y monitorear permanentemente los servicios prestados por terceros para cerciorarse que los servicios cumplen con la función para la que fueron contratados.

Para el cumplimiento de esta política es necesario realizar constantemente auditorías a los servicios que sean contratados de terceros, para verificar que se utilice únicamente información necesaria, que su funcionamiento sea el correcto y el que requiere la universidad.

Además, se debe monitorear el funcionamiento de los servicios, mantener un registro de la información que maneja, de los cambios o actualizaciones que se realice en los servicios, así como de asignar un responsable para chequear la adherencia de los servicios a los acuerdos firmados.

- Gestión de cambios en los servicios prestados por terceros.

Gestionar los cambios en los servicios prestados por terceros, el mantenimiento, procedimientos y controles de seguridad tomando en cuenta la criticidad de la información que manejan.

Para el cumplimiento de esta política es necesario mantener registrados los cambios, para mejorar los servicios, además del desarrollo, modificación o actualización de las políticas y procedimientos. Se debe implementar nuevos controles para robustecer la seguridad de la información.

Al momento de realizar los cambios en los servicios de terceros implementar mejoras y cambios en la infraestructura y red, adaptación, uso de nuevas tecnologías, productos, desarrollo de herramientas y nuevos ambientes de ser necesario cambio de la ubicación física de los medios del servicio.

4.2.13. Gestión de los incidentes en la seguridad de la información

El presente dominio tiene por objetivo gestionar los diversos incidentes tomando en cuenta que todos los activos de información con los que cuenta la universidad están expuestos a sufrir incidentes de seguridad, se debe garantizar la gestión de estos incidentes iniciando desde la comunicación, de forma que sean corregidos oportunamente. Para gestionar dichos incidentes es necesario la detección, comunicación, tratamiento y colaboración en la prevención de similares incidentes, para esto se requiere la colaboración de todo el personal de la universidad. Las políticas de seguridad establecidas en este dominio se basan en los controles publicados en el portal ISO “Gestión de los incidentes en la seguridad de la información” [27].

- Gestión de incidentes de seguridad de la información y mejoras

  - Responsabilidades y procedimientos.

La política de seguridad es asignar las responsabilidades y procedimientos, a cada uno de los funcionarios del área de sistemas y demás departamentos para identificar eficaz y rápidamente los incidentes de seguridad.

Para el cumplimiento de esta política es necesario que se capacite a todos los usuarios, sobre la utilización de los sistemas de información para que puedan informar adecuadamente sobre evento o debilidades que pueden afectar a la seguridad de la información.

El encargado de seguridad de la información es el responsable de aplicar los procedimientos necesarios para gestionar los incidentes y debilidades de la información de tipo: base de datos, infraestructura física, sistemas de información, servicios, equipos y software en cuanto se refiere a acceso o modificación no autorizada, destrucción o pérdida de información e inaccesibilidad.

  - Notificación de los eventos de seguridad de la información.

En cuanto a eventos de información suscitados, la política de seguridad es informar sobre los eventos de seguridad implementados o actualizados, lo antes posible mediante correos electrónicos y circulares a los encargados y empleados que utilizan los sistemas de información afectados.

Para el cumplimiento de esta política es necesario que el encargado de seguridad de la información informe, a los usuarios de los sistemas de información sobre los eventos de seguridad implementados o actualizados para evitar la creación de errores al manipular la información.

Se deberá informar vía correo electrónico institucional o mediante circulares a todos los usuarios afectados, de ser necesario realizar capacitaciones para la sociabilización de eventos de seguridad de la información.

- Notificación de puntos débiles de la seguridad.

En cuanto a puntos débiles, la política de seguridad es notificar cualquier tipo de evento o debilidad sospechosa que pueda afectar al funcionamiento normal de los sistemas de información.

Para el cumplimiento de esta política es necesario implementar una cuenta de correo para soporte, a la que se deberán notificar los eventos o debilidades sospechosas, con toda la información posible y los antecedentes del evento.

La administración de este correo lo deberá realizar el encargado de seguridad de la información, dependiendo de la gravedad del incidente, debe contactarse con la persona que reporta y con el encargado de sistemas de ese departamento o área en un plazo máximo de 48 horas, para recopilar la información necesaria para el análisis del evento, se debe llenar la plantilla para el tratamiento y valoración de incidentes que se encuentra en el ANEXO E.

Luego de la recolección de la información del incidente el encargado de seguridad de la información debe analizar los antecedentes.

- Valoración de eventos de seguridad de la información y toma de decisiones.

La política de seguridad es evaluar los eventos de seguridad de acuerdo al análisis realizado y tomar decisiones sobre la calificación del incidente.

Para el cumplimiento de esta política es necesario cumplir la política de notificación de puntos débiles de la seguridad, luego de realizar el análisis se puede tener las siguientes opciones de clasificación de los eventos:

- ✓ Corresponde a una amenaza: se informa al funcionario que reporto el evento sobre la amenaza y se cierra el registro.
- ✓ Corresponde a una debilidad: se realiza las actividades o procedimientos necesarios con el área o departamento y activos comprometidos, dejando constancia mediante el registro de la plantilla para el tratamiento y valoración de incidentes que se encuentra en el ANEXO E.
- ✓ Ocurrió y debe ser tratado como un incidente: se activa el proceso de gestión de incidentes, cumpliendo con todas los puntos de este dominio.

- Respuesta a los incidentes de seguridad.

La política de seguridad es que se debe proporcionar una respuesta inmediata ante los incidentes de información cumpliendo los procedimientos documentados.

Para el cumplimiento de esta política, la persona o área encargada debe dar respuesta a los incidentes, tiene un tiempo máximo de 48 horas para comunicarse con el funcionario que lo reporto y seguir con los procedimientos para su evaluación. Además, se debe desarrollar acciones inmediatas como:

- ✓ Coordinar los procedimientos o actividades necesarias para disminuir y evitar que se propaguen los daños o efectos del incidente.
- ✓ Reclasificar los eventos de acuerdo a la política de valoración de eventos de seguridad de la información y toma de decisiones.
- ✓ Mantener un registro de las evidencias recopiladas durante su gestión.
- ✓ Si el incidente afecta a organismos externos se debe notificar sobre el incidente.

- ✓ Mantener contacto con el administrador de los sistemas para gestionar la recuperación.
- ✓ Documentar los antecedentes relacionados con el incidente para saber los procedimientos a seguir si volviese a suceder.

- Aprendizaje de los incidentes de seguridad de la información.

En lo que se refiere a aprendizaje de incidentes, la política de seguridad es utilizar los conocimientos adquiridos en análisis y solución de incidentes de seguridad anteriores, con el fin de reducir el impacto en incidentes futuros.

Para el cumplimiento de esta política es necesario que la persona encargada de los incidentes de seguridad realice una revisión periódica de los incidentes atendidos en un periodo de tiempo. Para esta revisión se debe tomar en cuenta los incidentes recurrentes o de alto impacto en la información y problemas secundarios ocasionados.

Además se debe considerar la eficacia de la respuesta, solución y tratamiento dependiendo del tipo, volumen y costo de los incidentes. Uno de los puntos importantes es que el encargado de seguridad es el responsable de identificar, proponer a los miembros de la DITIC las medidas necesarias para mejorar o implementar controles de seguridad con el fin de minimizar incidencias de fallos o daños.

- Recopilación de evidencias.

La política de seguridad es, definir y aplicar procedimientos para mantener un registro de los incidentes para identificar y prevenir que vuela a suceder.

Para el cumplimiento de esta política es necesario que se cumplan todas las políticas de este dominio, y se debe documentar los incidentes de acuerdo a la plantilla para el tratamiento y

valoración de incidentes, la original deberá ser documentada y crear una bitácora digital de los incidentes y su solución para facilitar el acceso a la información y la búsqueda.

4.3. Elaboración de un plan de evaluación continua de seguridad de la información mediante responsabilidades y procedimientos.

El objetivo es evaluar continuamente la seguridad de la información para mantener sus principales características. Para el cumplimiento de este objetivo se desarrolla políticas de seguridad para asegurar la continuidad del negocio, y el cumplimiento de políticas anteriores.

4.3.1. Aspectos de seguridad de la información en la gestión de la continuidad del negocio

El objetivo de este dominio es, preservar la seguridad de la información durante las fases de activación y desarrollo de procesos, procedimientos y planes; incluyendo dentro de los procesos críticos la gestión de la seguridad referente a la legislación, personal, materiales, transporte e instalación de servicios adicionales. Las políticas establecidas en el presente dominio se basan en los controles publicados en el portal ISO "Aspectos de seguridad de la información en la gestión de la continuidad del negocio" [28].

- Continuidad de seguridad de la Información

  - Planificación de la continuidad de la seguridad de la información.

Para la planificación de la continuidad de la seguridad, la política de seguridad es determinar las necesidades y requisitos para la gestión de situaciones de crisis y desastres que afecten a la seguridad de la información.

Para el cumplimiento de esta política es necesario obtener el compromiso del encargado de la seguridad de la información para desarrollar un plan de continuidad. identificar y entender

los riesgos al que está expuesta la universidad y los activos de la información de acuerdo a la prioridad de los procesos en relación al impacto.

Se debe considerar el impacto que puede causar las interrupciones en el funcionamiento normal de los sistemas de información, en caso de suceder un evento de seguridad, considerar la utilización de pólizas de seguros en todo el proceso de continuidad del negocio y gestión de riesgos o la implementación de controles preventivos.

- Implantación de la continuidad de la seguridad de la información.

Para la implementación, la política de seguridad es identificar, documentar y ejecutar los procedimientos y controles para garantizar el nivel de seguridad de la información que requiera la universidad ante situaciones adversas.

Para el cumplimiento de esta política es necesario identificar recursos financieros, tecnológicos, ambientales, humanos para el tratamiento de los recursos adversos identificados, garantizando la seguridad del personal, cada uno de los planes deben ser documentados.

Se debe dar a conocer el plan completo, con responsabilidades, funcionalidades y actividades a seguir en caso de situaciones adversas a todo el personal que participe en el sistema de seguridad de la información.

- Verificación, revisión y evaluación de la continuidad de la seguridad de la información.

Verificar y evaluar periódicamente los controles de políticas de seguridad de continuidad del negocio, para que en caso de situaciones adveras estos controles sean eficaces y válidos.

Para el cumplimiento de esta política es necesario verificar los controles por lo menos una vez al año, se debe ejecutar pruebas que involucren a los usuarios asociados, para garantizar que tengan el conocimiento de cómo deben ser ejecutados los procedimientos y actividades necesarias para tratar las situaciones adveras.

Para realizar la evaluación de los controles es necesario simular de la forma más fidedigna posible con las consecuencias reales, para verificar la eficacia y realidad de los controles. El resultado debe ser registrado y de ser necesario tomar las acciones necesarias para mejorar.

- Redundancias

  - Disponibilidad de instalaciones para el procesamiento de información.

La política de seguridad es tener un área adecuada y con suficiente espacio para las instalaciones de procesamiento de información, para que la información mantenga su característica de disponibilidad.

Para el cumplimiento de esta política es necesario que se planifique y se realice planos antes de la creación de una nueva área de procesamiento de información, tomando en cuenta las nuevas tecnologías, y la posible implementación de nuevos equipos. Las instalaciones de procesamiento de información siempre deben estar aptas para la implementación de controles de seguridad o nuevas aplicaciones.

4.3.2. Cumplimiento

Las políticas detalladas en este documento deben ser cumplidas por todos los funcionarios que directa o indirectamente tengan contacto o procesen información. En especial los funcionarios que mantengan contacto directo con los sistemas de información. Todas las implementaciones de seguridad deben estar dentro de las normas legales que rigen a las

entidades educativas públicas. Se basan en los controles publicados por el portal ISO "Cumplimiento" [29].

- Cumplimiento de los requisitos legales y contractuales

  - Identificación de la legislación aplicable.

Para este control, la política de seguridad es identificar, documentar y mantener las normas y estatutos legales que involucran e intervienen en el cumplimiento de las políticas de seguridad.

Para el cumplimiento de esta política es necesario que se designe a una persona que se mantenga actualizada con las normas y estatutos legales que rigen en el país y la universidad en especial las que involucran tratamiento de información, correos electrónicos o tengan relación con la tecnología.

De realizarse algún cambio con las normas o estatutos del país o de la universidad, inmediatamente revisar si los controles de seguridad están dentro de los reglamentos y estatutos en caso de no estar, adaptar los controles para que no se incumpla con las leyes.

  - Derechos de propiedad intelectual (DPI).

En cuanto a derechos de propiedad intelectual, la política de seguridad es garantizar el cumplimento de los derechos de propiedad intelectual utilizando software original.
Para el cumplimiento de esta política es necesario que la persona encargada de las normas y estatutos también conozca los requisitos legislativos, normativos y contractuales de la propiedad intelectual tanto para nuevas creaciones e implementaciones de software. Además para la adquisición de servicios y software se debe garantizar que sean originales.

- Protección de los registros de la organización.

Para este control, la política de seguridad es proteger los registros de la organización contra acceso no autorizada, perdida, falsificación de acuerdo con los requisitos legales, normas y estatutos vigentes.

Para el cumplimiento de esta política es necesario mantener actualizada los reglamentos, normas y estatutos internos de la universidad en concordancia con los reglamentos nacionales y mundiales, es necesario que la persona encargada de este ámbito se encuentre informada, de ser necesario capacitarlo en aquellos reglamentos complejos que requieran de una capacitación.

- Protección de datos y privacidad de la información personal.

La política de seguridad es garantizar que la información personal de los empleados, docentes, funcionarios y estudiantes se encuentre protegida según los reglamentos y normativas pertinentes.

Para el cumplimiento de esta política es necesario que las bases de datos de la universidad debe estar protegida con usuarios y contraseñas, para asegurar los datos. Además que los equipos que utilizan los funcionarios de la universidad, deben estar protegidos contra accesos no autorizados, se debe cumplir con todos los niveles de seguridad contra acceso no autorizado.

- Regulación de los controles criptográficos.

La política de seguridad es, utilizar controles criptográficos para garantizar la seguridad de la información, de acuerdo con las normas, acuerdos y reglas pertinentes.

Para el cumplimiento de esta política es necesario que se implementen las políticas de seguridad que involucren controles criptográficos. Para de esta manera resguardad la información ante manipulación no autorizada, en especial la información calificada con nivel de criticidad alta. Previamente realizar un análisis el algoritmo de encriptación a utilizar.

- Revisiones de la seguridad de la información

  - Revisión independiente de la seguridad de la información.

Para la revisión individual de la seguridad, la política de seguridad es identificar las políticas de seguridad establecidas en el presente documento que van a ser aplicadas a la universidad dependiendo de las necesidades.

Para el cumplimiento de esta política es necesario que se realice un análisis de las políticas necesarias para preservar los niveles de seguridad de la información. Este análisis debe ser realizado por la DITIC, el que debe arrojar como resultado las políticas de seguridad que se deben aplicar, tomando en cuenta la criticidad de la información, el nivel de acceso, la ubicación física de los equipos.

  - Cumplimiento de las políticas y normas de seguridad.

La política de seguridad es que el encargado del área de sistemas de cada departamento y facultad, es el encargado de realizar revisiones periódicas del cumplimiento de los procesos y procedimientos de las políticas de seguridad del departamento a su cargo.

Para el cumplimiento de esta política es necesario que el encargado del área de sistemas de cada departamento y facultad, revisar periódicamente el cumplimiento de los procedimientos necesarios respecto a las políticas de seguridad de la información, normas o estatutos que rigen dentro de la universidad.

- Comprobación del cumplimiento

La política de seguridad es verificar que los sistemas de información cumplan con las políticas de seguridad identificadas para ser aplicadas dentro de la universidad.

Para el cumplimiento de esta política es necesario que se realicen pruebas de los sistemas de información para verificar que se cumplan las políticas de seguridad, que se aplican dentro de la universidad. Para asegurar la integridad, confiabilidad y disponibilidad de la información. Además de proteger la información de estudiantes, docentes y personal que pertenecen a la UTA.

CAPÍTULO V

5. CONCLUSIONES Y RECOMENDACIONES

5.1.Conclusiones

- Al realizar la presente investigación se pudo determinar que el activo más importante de cada organización es la información, por lo tanto es importante protegerla para lo cual una adecuada norma de protección es fundamental para evitar modificaciones o accesos no autorizados.

- El personal administrativo, docentes y estudiantes realizan sus funciones acorde a la información que brindan los sistemas de la universidad, por lo tanto, es importante que la información y centros de procesamiento tengan restringido el acceso, estableciendo lineamientos de seguridad para la información en base a la norma ISO 27002, que ayuda a protegerla, puesto que las políticas de seguridad minimizan el riesgo de pérdida de información garantizando el correcto funcionamiento de los procesos.

- La tecnología cada día cambia, por esta razón la universidad debe estar constantemente actualizada en los ámbitos de tecnología, telecomunicaciones y políticas de seguridad, aplicando procedimientos, documentación y manuales para la estandarización de los procesos.

5.2.Recomendaciones

- Se debe realizar una campaña de capacitación a los usuarios involucrados en los procesos, para crear una cultura de colaboración y asistencia en la seguridad, así como para la implementación de futuras mejoras dentro de la universidad.

- La DITIC debe profundizar el conocimiento de la Norma ISO 27002, para contar con la asistencia de personal capacitado y certificado en este estándar; se debe tomar en cuenta las diversas amenazas a los activos y aplicar las políticas necesarias para mitigar el riesgo al que está expuesto funcionamiento del activo.

- Se debe formalizar el documento de políticas de seguridad para su aprobación por el consejo universitario y la difusión de las mismas a todos los funcionarios y empleados de la institución, de modo que se cree conciencia sobre la importancia de la información y se mantenga un estricto control en los cambios de software, acceso al código fuente para evitar el plagio de información y de sistemas desarrollados dentro de la universidad.

BIBLIOGRAFÍA

[1] Norma de Seguridad Informática ISO 27001 para mejorar la confiabilidad, integridad y disponibilidad de los sistemas de información y comunicación en el Departamento de Sistemas de la Cooperativa de Ahorro y Crédito San Francisco LTDA., [Online]. Universidad Técnica de Ambato. Disponible en: http://repo.uta.edu.ec/bitstream/handle/123456789/2361/Tesis_t715si.pdf?sequence=1.

[2] Análisis e Implementación de la norma ISO 27002 para el departamento de sistemas de la Universidad Politécnica Salesiana sede Guayaquil, [Online]. Universidad Politécnica Salesiana sede Guayaquil. Disponible en: http://dspace.ups.edu.ec/bitstream/123456789/3163/1/UPS-GT000319.pdf.

[3] Plan maestro de Seguridad Informática para la UTIC de la ESPE con lineamientos de la norma ISO/IEC 27002", [Online]. Escuela Politécnica del Ejército. Disponible en: http://repositorio.espe.edu.ec/bitstream/21000/6025/1/T-ESPE-034491.pdf.

[4] Purificación Aguilera, *Seguridad Informática*, 1ra ed. Editex, Seguridad Informática, 2010, pp. 9.

[5] Purificación Aguilera, *Seguridad Informática*, 1ra ed. Editex, Tipos de Seguridad, 2010, pp. 9.

[6] Carmen de Pablos, *Organización y transformación de los sistemas de información en empresas,* 1ra ed. Universidad Rey San Carlos, 2011,pp. 360.

[7] Directorio de la norma ISO 27000. [Online]. Disponible en: http://www.27000.org/iso-27002.htm.

[8] El portal de ISO 27001 en Español. [Online]. Disponible en: http://www.iso27000.es/iso27000.html [Accedido: Mayo. 18, 2014].

[9] ISO 27002:2013 [Online]. Disponible en: http://www.iso27000.es/download/ControlesISO27002-2013.pdf [Accedido: Mayo. 18, 2014].

[10] ISO 27000.es, "El portal de ISO 27001 en Español", [Online]. Disponible en: http://iso27000.es/glosario.html [Accedido: Mayo. 18, 2014].

[11] Carla Rodríguez Salas. (2002). Gestión de la Información e las Organizaciones, *Bibliotecas*, vol. XX (1 y 2), pp. 19-34.

[12] Galende Díaz Juan Carlos, *Criptografía Historia de la escritura cifrada*, 1ra ed., Editorial Complutense, 1995, pp. 15.

[13] Martínez Juan Gaspar, *Planes de contingencia*, 1ra ed., Editorial Díaz de Santo S.A., 2004, pp. 28.

[14] UTA, "*DITIC*", [Online]. Disponible en: www.uta.edu.ec.

[15] Acuerdo de Confidencialidad [Online]. Disponible en: http://www.jcyl.es/web/jcyl/binarios/982/337/Modelo%20Contrato%20de%20Confidencialidad.doc?blobheader=application/msword&blobnocache=true

[16] ISO 27000.es, "Políticas de Seguridad", [Online]. Disponible en: http://iso27000.es/iso27002_5.html.

[17] ISO 27000.es, "Aspectos organizativos de la seguridad de la información", [Online]. Disponible en: http://iso27000.es/iso27002_6.html.

[18] ISO 27000.es, “Seguridad ligada a los recursos humanos”, [Online]. Disponible en: http://iso27000.es/iso27002_7.html.

[19] ISO 27000.es, “Gestión de activos”, [Online]. Disponible en: http://iso27000.es/iso27002_8.html.

[20] ISO 27000.es, “Control de acceso”, [Online]. Disponible en: http://iso27000.es/iso27002_9.html.

[21] ISO 27000.es, “Cifrado”, [Online]. Disponible en: http://iso27000.es/iso27002_10.html.

[22] ISO 27000.es, “La seguridad física y ambiental”, [Online]. Disponible en: http://iso27000.es/iso27002_11.html.

[23] ISO 27000.es, “Seguridad en la operativa”, [Online]. Disponible en: http://iso27000.es/iso27002_12.html.

[24] ISO 27000.es, “Seguridad en las telecomunicaciones”, [Online]. Disponible en: http://iso27000.es/iso27002_13.html.

[25] ISO 27000.es, “Adquisición, desarrollo y mantenimiento de los sistemas de información”, [Online]. Disponible en: http://iso27000.es/iso27002_14.html.

[26] ISO 27000.es, “Relaciones con suministradores”, [Online]. Disponible en: http://iso27000.es/iso27002_15.html.

[27] ISO 27000.es, “Gestión de los incidentes en la seguridad de la información”, [Online]. Disponible en: http://iso27000.es/iso27002_16.html.

[28] ISO 27000.es, “Aspectos de seguridad de la información en la gestión de la continuidad del negocio”, [Online]. Disponible en: http://iso27000.es/iso27002_17.html.

[29] ISO 27000.es, “Cumplimiento”, [Online]. Disponible en: http://iso27000.es/iso27002_18.html.

ANEXOS

ANEXO A

Inventario de Hardware y Software de los computadores

Nombre del equipo	
Dirección IP	
Mascara de Subred	
Nombre de Dominio	
Ubicación Física del Equipo	
Modelo Procesador	
Marca	
Modelo	
Numero de Procesadores	
Velocidad Procesador	
Sistema Operativo	
Versión de Sistema Operativo	
Memoria RAM	
Capacidad de Almacenamiento	
Seriales de los componente	

Lineamientos de uso de los equipos

- ✓ Cerca de los equipos, no ingerir alimentos y bebidas.
- ✓ No fumar cerca de los equipos.
- ✓ Mantener conectado a un regulador de voltaje para evitar variaciones de voltaje.
- ✓ No insertar objetos en las ranuras de los equipos.
- ✓ No realizar cambios o actividades de mantenimiento sobre el hardware.
- ✓ Conservar los equipos bajo adecuadas condiciones ambientales.
- ✓ Apagar los equipos que no estén en uso.

ANEXO B

Formulario de Solicitud de acceso a Sistemas de Información

Solicitud de acceso a Sistemas de Información	
1. Datos Generales	
Campus:	
Facultad:	
Departamento:	
2. Datos del usuario	
Apellido y Nombre del solicitante:	
Cargo:	Telf.:
Correo Electrónico:	

3. Perfil de usuario a crear o modificar	
Sistema de Información:	
Creación	**Modificación**
Perfil Nº ☐	Eliminación: ☐
Perfil Nº ☐	Cambio perfil: ☐
	Elaboración: ☐
	Revisión: ☐
	Aprobación: ☐

4. Firmantes

_____	_____
Cargo:	Cargo:
Fecha:	Fecha:
Solicitante	Autorizado

5. Aprobación (Para uso Interno Coordinación)

_____

Cargo:
Fecha:
Aprobación

Observación:

- ✓ El usuario y la contraseña son de uso personal por ningún motivo se debe divulgar esa información.
- ✓ En caso de que el funcionario sea suspendido temporal o definitivamente, se debe informar de inmediato al administrador de usuarios.
- ✓ En caso que se realice cambios en perfiles de usuarios, se debe informar de inmediato al administrador de usuarios.
- ✓ El funcionario propietario del usuario es responsable de todos los cambias realizados en los sistemas de información.
- ✓ El funcionario debe salir de los sistemas de información si no está realizando ninguna tarea.

ANEXO C

Formulario de Creación de usuario y responsabilidad de contraseñas

Solicitud de acceso a Sistemas de Información	
1. Datos Generales	
Campus:	
Facultad:	
Departamento:	
2. Datos del usuario	
Apellido y Nombre del solicitante:	
Cargo:	Telf.:
Correo Electrónico:	

3. Perfil de usuario a crear	
Sistema de Información:	
Usuario	
Contraseña	

4. Obligaciones de usuario

- ✓ La información como clave y contraseña es de uso personal y no puede ser otorgado a otro funcionario por ningún motivo.
- ✓ Para cambios de perfiles de usuario se debe comunicar al área de seguridad de la información.
- ✓ Si un funcionario es suspendido temporánea o definitivamente se debe comunicar al área de seguridad de la información para su respectiva desactivación.
- ✓ El funcionario es responsable de todas las operaciones realizadas en los sistemas de información con el usuario y contraseña otorgados.
- ✓ El funcionario debe cerrar su sesión de usuario cuando este no esté en uso.

5. Firmantes

_____	_____
Cargo:	Cargo:
Fecha:	Fecha:
Solicitante	Autorizado

ANEXO D

Listado de servidores y contraseñas

Solicitud de acceso a Sistemas de Información	
1. Datos Generales	
Campus:	
Facultad:	
Departamento:	
2. Datos del usuario	
Apellido y Nombre del solicitante:	
Cargo:	Telf.:
Correo Electrónico:	

3. Listado de servidores

HOSTNAME	DIRECCION IP	USUARIO	CONTRASEÑA

4. Firmantes

_____	_____
Cargo:	Cargo:
Fecha:	Fecha:
Solicitante	Autorizado

ANEXO E

Plantilla para el Tratamiento y Valoración de incidentes

Tratamiento y Valoración de incidentes	
1. Datos Generales	
Facultad o Departamento:	
Quien lo reporta:	
Número de incidente:	
Prioridad:	
Usuarios afectados:	
2. Datos del incidente	
Descripción del incidente:	
Posible causa:	
Fecha y hora aproximada que comenzó:	
Fecha y hora de detección:	
Fecha y hora de restauración:	
Sistemas Afectados	
Registros/Datos afectados:	

Protocolos atacados (HTTP, SIMP, POP, etc.):	
Objetivo de sistema afectado:	
Costos asociados:	
Actividades de restauración:	
Resolución:	

3. Firmantes

_____	_____
Cargo:	Cargo:
Fecha:	Fecha:
Solicitante:	Responsable: