UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS

Tema:

"Análisis e Implantación de la norma ISO/IEC 27002:2013 para el departamento informático del Gobierno Autónomo Descentralizado Municipal del Cantón Salcedo".

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

SUBLÍNEA DE INVESTIGACIÓN: Seguridad de Unidades Informáticas.

AUTOR: Sandra Maribel Criollo Tasinchana.
TUTOR: Ing. Franklin Oswaldo Mayorga Mayorga.

Ambato – Ecuador
Octubre – 2017

APROBACIÓN DEL TUTOR

En mi calidad de Tutor del Trabajo de Investigación sobre el Tema: **"Análisis e Implantación de la norma ISO/IEC 27002:2013 para el departamento informático del Gobierno Autónomo Descentralizado Municipal del Cantón Salcedo",** de la Señorita Sandra Maribel Criollo Tasinchana, 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 Octubre, 2017

EL TUTOR

Ing. Franklin Oswaldo Mayorga Mayorga.

AUTORÍA

El presente trabajo de investigación titulado: **"Análisis e Implantación de la norma ISO/IEC 27002:2013 para el departamento informático del Gobierno Autónomo Descentralizado Municipal del Cantón Salcedo".** 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 Octubre, 2017

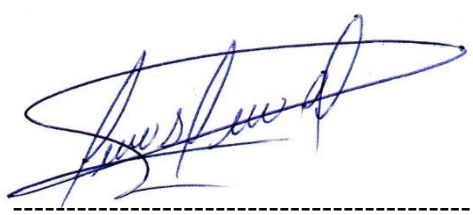
Sandra Maribel Criollo Tasinchana
CC: 0503225344

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 Octubre, 2017



Sandra Maribel Criollo Tasinchana
CC: 0503225344

APROBACIÓN DE LA COMISIÓN CALIFICADORA

La Comisión Calificadora del presente trabajo conformada por los señores docentes Ing. Dennis Vinicio Chicaiza Castillo e Ing. Carlos Israel Nuñez Miranda, revisó y aprobó el Informe Final del Proyecto de Investigación titulado **"Análisis e Implantación de la norma ISO/IEC 27002:2013 para el departamento informático del Gobierno Autónomo Descentralizado Municipal del Cantón Salcedo"**, presentado por la señorita Sandra Maribel Criollo Tasinchana 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.

Ing. Mg. Elsa Pilar Urrutia Urrutia
PRESIDENTA DEL TRIBUNAL

Ing. Dennis Vinicio Chicaiza Castillo
DOCENTE CALIFICADOR

Ing. Carlos Israel Núñez Miranda
DOCENTE CALIFICADOR

DEDICATORIA:

Con mucho amor dedico este trabajo a mi Madre Ana Maria Tasinchana por su apoyo incondicional y ánimos para no desmayar en ningún momento de esta etapa, gracias por sembrar en mí valores y formar mi carácter y persona.

A mi Padre Abelardo Criollo por su ayuda en el transcurso de mi carrera estudiantil. A mis hermanas por su cariño y ayuda.

De manera especial a mi futuro esposo Milton José Tenorio Eusebio por sus palabras de aliento diario, apoyo, inspiración y presencia en mi vida.

Sandra Maribel Criollo Tasinchana

AGRADECIMIENTO:

Agradezco en primer lugar a Dios por haberme dado la vida y salud para disfrutar de tantos momentos hermosos de mi vida, como la satisfacción de la tarea cumplida.

A la Facultad de Ingeniería en Sistemas Electrónica e Industrial por acogerme y formarme como una profesional.

De manera especial a mi tutor Ing. Franklin Mayorga, por su ayuda y guía importante para concluir este trabajo, gracias a su dirección y apoyo.

Sandra Maribel Criollo Tasinchana

PAGINAS PREIMINARES

ÍNDICE

CAPITULO IV

DESARROLLO DE LA PROPUESTA

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

INDICE DE GRAFICOS

Resumen

En el proyecto de investigación se presenta la experiencia obtenida en la aplicación de técnicas a fin de obtener información acerca de la norma ISO/IEC 27002:2013 en las organizaciones gubernamentales donde el objetivo es desarrollar habilidades que beneficie a la infraestructura tecnológica y humana dentro de la edificación protegiendo la seguridad de la información. Por lo que se llevó a cabo un análisis de encuestas, entrevistas para obtener los efectos que causan el manejo de la información sin una estrategia planificada de tal manera que, los resultados deben ajustarse a los estándares utilizados en la investigación para mejorar el rendimiento del personal que labora dentro de la organización; Se realizó un análisis dentro de la infraestructura tecnológica de la Institución donde se observó muchas falencias en cuanto al manejo de la información y mediante la investigación se estableció un plan estratégico para corregirlas y con esto lograr impulsar los controles de seguridad para que sean integrados acorde a las necesidades de la organización.

Abstract

This proyect of investigation presents the experience obtained in the application of techniques to obtain information about ISO / IEC 27002: 2013 in governmental organizations where the objective is to develop skills that benefit the technological and human infrastructure within the building Protecting the security of information. So we conducted a survey analysis, interviewing to obtain the effects that cause the management of information without a planned strategy in such a way that the results should conform to the standards used in research to improve staff performance That works within the organization; An analysis was made within the technological infrastructure of the Institution where there were many shortcomings in terms of information management and through the investigation a strategic plan was established to correct them and with this, to promote the security controls so that they are integrated according to The needs of the organization.

INTRODUCCIÓN

El presente trabajo de investigación **"Análisis e Implantación de la norma ISO/IEC 27002:2013 para el Departamento Informático del Gobierno Autónomo Descentralizado Municipal del Cantón Salcedo.",** consta de cinco capítulos los cuales se detallan a continuación:

Capítulo I. "El Problema", se identifica el problema que se suscita en un contexto de la realidad, para plantearlo de forma concreta, delimitando el alcance, con una respectiva justificación y el planteamiento de los objetivos que guiarán todo el proyecto.

Capítulo II. "Marco Teórico", consta del fundamento teórico que ayuda a comprender de forma clara el problema gracias a los antecedentes investigativos, para luego plantear la propuesta de solución.

Capítulo III. "Metodología", Se describe las metodologías de investigación que se utilizarán, el enfoque, la modalidad de la investigación utilizada, el tipo de investigación realizada.

Capítulo IV. "Desarrollo de la Propuesta", en este capítulo se describe todo el desarrollo de la solución, definiendo los requisitos necesarios, los criterios que se aplicaron dando como resultado el plan estratégico.

Capítulo V. "Conclusiones y Recomendaciones", estableciendo las conclusiones a las que llega el investigador luego del desarrollo del proyecto, así también las recomendaciones pertinentes.

Finalmente se incluye las referencias citadas en este documento, en los anexos se incluye los instrumentos utilizados para la recolección de la información correspondientes del presente proyecto.

CAPÍTULO I

EL PROBLEMA

1.1 El Tema

"ANÁLISIS E IMPLANTACIÓN DE LA NORMA ISO/IEC 27002:2013 PARA EL DEPARTAMENTO INFORMÁTICO DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN SALCEDO."

1.2 Planteamiento del problema.

La evolución de la información, tecnología y métodos para vulnerar sistemas informáticos de los entes gubernamentales han puesto en alerta a las organizaciones internacionales dedicadas a la seguridad con el fin de proteger la información dentro de estas a través de normas, las organizaciones se encuentran en una etapa, donde se han generado amenazas, variantes de malware, ataques dirigidos, La inadecuada inversión en dispositivos, aplicaciones y ausencia de normas de seguridad, da paso a vulnerabilidades que provocan la pérdida de información mediante infiltraciones de intrusos en los equipos conectados a la red, por lo cual es necesario realizar un análisis de estas amenazas en un contexto general, con las principales causas que puedan ocasionar los incidentes que las normas y estándares internacionales proporcionan los mecanismos de seguridad garantizados en un rendimiento más óptimo en cuanto a la seguridad de un departamento informático para aumentar la confianza dentro del mismo a los proveedores, socios de negocio y empleados de manera sustentable.

I-SEC del Ecuador ofrece sus servicios para que las empresas puedan implementar el SGSI- 27000, partiendo de un análisis inicial respecto al nivel de cumplimiento de la empresa (existencia de controles) referente a los controles propuesto por ISO 27001 / 27002, para luego desarrollar estrategias que permitan disminuir la brecha existente entre la situación inicial de la empresa y la situación anhelada según el enfoque ISO 27000 [1].

En Ecuador, varios entes públicos y privados contextualizan a la información como un problema tecnológico, ya es tiempo de replantear los programas de seguridad de la información y las estrategias que las compañías deben utilizar para mantener a salvo sus activos más valiosos. La seguridad de la información debe estar alineada estratégicamente con la agenda de negocios más general y basarse en la tolerancia al riesgo de una organización [2].

En el año 2016 en el Gobierno Autónomo Descentralizado Municipal del Cantón Salcedo existen amenazas tanto dentro como fuera de la organización. La tecnología móvil, computación en nube, las redes sociales y el sabotaje por parte de los empleados son solo algunas de las amenazas internas que enfrentan las empresas, no cuentan con el personal o la tecnología para investigar debilidades y nuevos métodos de invasión a la infraestructura informática y de telecomunicaciones, de cómo estar prevenido y enfrentar a los ataques informáticos, esto provoca que personas maliciosas obtengan acceso a la información del GAD Municipal, con la utilización de herramientas tecnologías de información se podrá identificar los riesgos reales para evaluar las amenazas y aplicar los dominios de las normas de seguridad asegurando las funciones del gobierno para que sean las más adecuadas midiendo los indicadores principales para poder identificar los problemas cuando sean pequeños y sustentar el programa que desempeña el mismo garantizando la seguridad de la información [2].

1.3 Delimitación del problema.

Área Académica: Administrativas Informáticas.
Línea de Investigación: Normas y Estándares.
Sub líneas de investigación: Seguridad de Unidades Informáticas.
Delimitación Espacial: La presente investigación se desarrollará en el GAD Municipal del Cantón Salcedo.
Delimitación Temporal: La presente investigación se desarrollará durante el periodo académico Abril/2016-Septiembre/2017.

1.4 Justificación.

En la actualidad la seguridad de la información es muy necesaria ya que es vital para las organizaciones mantener la información recaudada y procesada a diario segura para el equilibrio de la misma que mantendrá el crecimiento económico y leal de esta, existen normativas, reglas y a través de estas se establece un sistema de gestión de seguridad de la información ya que este conjunto de estándares se reflejara para proteger dicho activo ante las constantes amenazas que surgen día tras día, esta norma se aplicara en el Departamento de informática del GAD Municipal del Cantón Salcedo en sus equipos tecnológicos actuales se podrá trabajar con la seguridad de la información de manera ordenada para el inicio del proceso.

Con la norma ISO/ICE 27002:2013 nos podremos establecer políticas y procedimientos para la aplicación del Sistema de gestión de la seguridad de la información, esta proporciona una amplia visión de los problemas de seguridad en cuanto a la información y recurso humano encargado de gestionarla, además de ser un estándar internacional proporciona dominios y controles que buscan optimizar los peligros o riesgos que tiene expuesto una organización, ya que es una obligación que está debe estar en los entes gubernamentales implementar la seguridad de la información, por la fuga de información que se puede reflejar

en las misma es por eso que, estas normativas serán las más adecuadas para empezar la acciones en las instituciones descentralizadas.

El presente proyecto de implantación de normas ISO, es importante ya que se podrá minimizar los inconvenientes de la seguridad, que tiene el Departamento de informática del GAD Municipal del Cantón Salcedo al momento procesar información, el beneficiario principal será el GAD Municipal del Cantón Salcedo, los encargados de los usuarios, ya que tendrá un impacto positivo y eficiente. Se tratará de llevar un enfoque directo hacia la información recauda, la razón es que muchos entes públicos a nivel provincial ya están iniciando planes de normas de seguridad, empresas y otras instituciones, en el Ecuador existen organizaciones.

1.5 Objetivos.

1.5.1 Objetivo General.

Realizar el análisis y la implantación de la norma ISO/IEC 27002:2013 en el Departamento Informático del Gobierno Autónomo Descentralizado Municipal del Cantón Salcedo.

1.5.2 Objetivos Específicos.

- Determinar la existencia de políticas de seguridad informática en el Departamento de informática del GAD Municipal del Cantón Salcedo para verificar los mecanismos de defensa internos y externos.
- Analizar los riesgos para determinar los controles necesarios ante las amenazas y sus vulnerabilidades a través de la norma ISO/IEC 27002:2013.
- Garantizar el cumplimiento independiente de los controles internos y requisitos de gestión corporativa, así como la continuidad de las actividades en el Departamento de informática del GAD Municipal del Cantón Salcedo.

- Implantar la norma ISO/IEC 27002:2013 en el Departamento de informática del GAD Municipal del Cantón Salcedo para cumplir con integridad, confidencialidad y disponibilidad de la información dentro del mismo.

CAPÍTULO II

MARCO TEÓRICO

2.1 Antecedentes investigativos.

Elizabeth Magdalena Torres Núñez, en su proyecto de investigación realizado en la Universidad Técnica de Ambato en su conclusión afirma que: 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 [3].

La seguridad informática permite proteger la infraestructura computacional incluyendo la información contenida, por ello debe ser tratada con la mayor responsabilidad en todas las áreas del departamento de sistemas, siendo uno de los factores de éxito principales la comunicación en la organización, porque el recuero humano organizado con normas y políticas establecidas más las herramientas computaciones colaboran en la prevención de amenazas y disminución de riesgos en seguridad [4].

El Contexto de la seguridad de la información en constante cambio, obliga a quienes gestionan en este campo a estar en constante actualización, por lo que se recomienda revisar la información: de alianzas estratégicas, normativas, marcos de referencia y con énfasis el marco legal local e internacional en el contexto de la seguridad de la información, sitios web en las que se reportan

nuevas vulnerabilidades y sitios en las que se publican sitios que fueron alterados la confidencialidad, integridad y disponibilidad [5].

Es necesario implementar el modelo de gestión de seguridad de información institucional como parte de la planificación estratégica a través de un objetivo estratégico puntual, que permita a su vez la generación de varios proyectos alineados, entre los cuales debe constar un POA dentro del área de TI en coordinación con el área financiera para mejorar los procesos críticos en función de la seguridad de información [6].

2.2 Fundamentación Teórica.

Seguridad

La información es hoy en día uno de los activos más importantes de las organizaciones, y debe protegerse.

La información y todos los soportes que la sustentan en una organización (sistemas y redes) están sometidos cada vez a más amenazas desde más fuentes.

Las clásicas amenazas: fraude, espionaje, sabotaje, vandalismo, fuego, inundaciones, etc.

Las nuevas amenazas: virus, hackers, negación de servicio, etc.

Las organizaciones dependen cada día más de sus sistemas de información, y son más vulnerables.

La mayoría de los SI no han sido diseñados con criterios de seguridad [7].

Tipos de Seguridad

Activa

“Comprende el conjunto de defensas o medidas cuyo objetivo es evitar o reducir los riesgos que amenazan al sistema.” “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.”

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.” [8].

SGSI

El SGSI es la abreviatura usada para referirse al Sistema de Gestión de la Seguridad de la Información e ISMS son las siglas equivalentes en ingles a Information Security Management System.

El Sistema de Gestión de Seguridad de la Información, según ISO 27001 consiste en preservar la confidencialidad, integridad y disponibilidad, además de todos los sistemas implicados en el tratamiento dentro de la organización.

El SGSI (Sistema de Gestión de Seguridad de la Información) es el principal concepto sobre el que se conforma la norma [9].
La secretaria nacional de administración pública, considerando que las TIC son herramientas imprescindibles para el desempeño institucional e inter-institucional, y como respuesta a la necesidad gestionar de forma eficiente y eficaz la seguridad de la formación en las entidades públicas, emitió los acuerdos ministeriales No. 804 y No. 837, de 29 de julio y 19 de agosto de 2011

respectivamente, mediante los cuales creo la comisión para la seguridad informática y de las tecnologías de la información y comunicación [10].

Sobre la ISO 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.”

“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.”

“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”. [11]

ISO 27001.

Un Sistema de Gestión de la Seguridad de la Información (SGSI), definido por la norma ISO/IEC 27001, no sólo debe considerar el contexto de la industria y características culturales de la Organización, sino que también debe ser sostenible en el tiempo, con capacidad de incorporar mejoras de forma incremental y continua, con un beneficio comprobable para la Organización. Para

ello se requiere de una metodología bien definida que acompañe el dinamismo necesario de la empresa/Organización y de la industria y a su vez respete las estrategias empresariales y vinculación estructural [12].

Esta norma, forma parte de la familia SGSI (Sistema de Gestión de la Seguridad de la información), INEN-ISO/IEC 27000, la cual tiene por objetivo común, la correcta creación y gestión del SGSI en una organización.

La norma ISO/IEC 27002, es un conjunto de recomendaciones de buenas prácticas enfocadas a una adecuada gestión de la seguridad de la información. Esta norma parte de la familia de normas SGSI la cual tiene por objetivos la correcta creación y gestión del SGSI en un ente organizacional.

La norma ISO/IEC 27002, es un conjunto de recomendaciones de buenas prácticas enfocadas a una adecuada gestión de la seguridad de la información. Esta contiene varios dominios, objetivos de control y controles, dependiendo de la edición, que sirven de guía al personal de una organización para iniciar, implantar y mantener SGSI.

Objetivos de la norma ISO 27002.

- Servir de punto de información de la serie de normas ISO 27000 y de la gestión de seguridad de la información mediante la aplicación de controles óptimos a las necesidades de las organizaciones en cada momento.
- Realizar la libre difusión de información en base a las investigaciones, conocimientos y búsquedas de los editores de la web.
- Responder a todas las consultas recibidas en relación a las normas de la serie ISO 27000, independientemente de su origen.
- Establecer contactos con todo tipo de organizaciones, desarrolladores y personas relacionadas con la norma, con el objetivo de intercambiar información, opiniones, experiencias o conocimientos, e impulsar la colaboración en

actividades de fomento y promoción de las buenas prácticas para la aplicación de controle para la seguridad de la información.

Especificación de dominios de la ISO 27002

1. **Políticas Seguridad.**

El contenido de las políticas se basa en el contexto en el que opera una organización y suelen ser considerados en su redacción los fines y objetivos de la organización, las estrategias adoptadas para alcanzar sus objetivos, la estructura y los procesos adoptados por la organización, los objetivos generales y específicos relacionados con el tema de la política y requisitos de las políticas procedentes de niveles más superiores relacionadas.

1.1. Directrices de la Dirección en seguridad de la información.

La gerencia debería establecer de forma clara las líneas de las políticas de actuación y manifestar su apoyo y compromiso a la seguridad de la información, publicando y manteniendo políticas de seguridad en toda la organización.

2. **Aspectos Organizativos SI.**

Las protecciones físicas de las organizaciones son cada vez más reducidas por las actividades de la organización requiere por parte del personal interno/externo que acceden a información desde el exterior en situación de movilidad temporal o permanente. En estos casos se considera que la información puede ponerse en riesgo si el acceso se produce en el marco de una inadecuada administración de la seguridad, por lo que se establecerán las medidas adecuadas para la protección de la información.

2.1. Organización interna.

La gerencia debería establecer de forma clara las líneas de la política de actuación y manifestar su apoyo y compromiso a la seguridad de la información, publicando y manteniendo una política de seguridad en toda la organización.

Se debería establecer una estructura de gestión con objeto de iniciar y controlar la implantación de la seguridad de la información dentro de la Organización.

El órgano de dirección debería aprobar la política de seguridad de la información, asignar los roles de seguridad y coordinar y revisar la implantación de la seguridad en toda la Organización.

3. Seguridad Ligada a los recursos humanos.

El objetivo del presente dominio es la necesidad de educar e informar al personal desde su ingreso y en forma continua, cualquiera sea su situación de actividad, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad y asuntos de confidencialidad.

Es necesario reducir los riesgos de error humano, comisión de actos ilícitos, uso inadecuado de instalaciones y recursos y manejo no autorizado de la información, junto a la definición de posibles sanciones que se aplicarán en caso de incumplimiento.

Se requiere explicitar las responsabilidades en materia de seguridad en la etapa de reclutamiento de personal e incluirlas en los acuerdos a firmarse y verificar su cumplimiento durante el desempeño del individuo como empleado, así como, garantizar que los usuarios estén al corriente de las amenazas e incumbencias en materia de seguridad de la información, y se encuentren capacitados para

respaldar la Política de Seguridad de la organización en el transcurso de sus tareas normales.

3.1. Antes de la contratación.

Las responsabilidades de la seguridad se deberían definir antes de la contratación laboral mediante la descripción adecuada del trabajo y los términos y condiciones del empleo.

Todos los candidatos para el empleo, los contratistas y los usuarios de terceras partes se deberían seleccionar adecuadamente, especialmente para los trabajos sensibles.

Los empleados, contratistas y usuarios de terceras partes de los servicios de procesamiento de la información deberían firmar un acuerdo sobre sus funciones y responsabilidades con relación a la seguridad.

3.2. Durante la contratación.

Se debería definir las responsabilidades de la Dirección para garantizar que la seguridad se aplica en todos los puestos de trabajo de las personas de la organización.

A todos los usuarios empleados, contratistas y terceras personas se les debería proporcionar un adecuado nivel de concienciación, educación y capacitación en procedimientos de seguridad y en el uso correcto de los medios disponibles para el procesamiento de la información con objeto de minimizar los posibles riesgos de seguridad.

3.3. Cese o cambio de puesto de trabajo.

Se deberían establecer las responsabilidades para asegurar que el abandono de la organización por parte de los empleados, contratistas o terceras personas se controla, que se devuelve todo el equipamiento y se eliminan completamente todos los derechos de acceso.

4. Gestión Activos.

El objetivo del presente dominio es que la organización tenga conocimiento preciso sobre los activos que posee como parte importante de la administración de riesgos.

Los activos de información deben ser clasificados de acuerdo a la sensibilidad y criticidad de la información que contienen o bien de acuerdo a la funcionalidad que cumplen y rotulados en función a ello, con el objeto de señalar cómo ha de ser tratada y protegida dicha información.

Las pautas de clasificación deben prever y contemplar el hecho de que la clasificación de un ítem de información determinado no necesariamente debe mantenerse invariable por siempre, y que ésta puede cambiar de acuerdo con una política predeterminada por la propia organización. Se debería considerar la cantidad de categorías a definir para la clasificación dado que los esquemas demasiado complejos pueden tornarse engorrosos y antieconómicos o resultar poco prácticos.

4.1. Responsabilidad sobre los activos.

Todos los activos deberían ser justificados y tener asignado un propietario y se deberían identificar a los propietarios para todos los activos y asignarles la responsabilidad del mantenimiento de los controles adecuados.

La implantación de controles específicos podría ser delegada por el propietario convenientemente. No obstante, el propietario permanece como responsable de la adecuada protección de los activos.

4.2. Clasificación de la información.

Se debería clasificar la información para indicar la necesidad, prioridades y nivel de protección previsto para su tratamiento.

4.3. Manejo de los soportes de almacenamiento.

Los medios deberían ser controlados y físicamente protegidos.

Se deberían establecer los procedimientos operativos adecuados para proteger los documentos, medios informáticos (discos, cintas, etc.), datos de entrada o salida y documentación del sistema contra la divulgación, modificación, retirada o destrucción de activos no autorizadas.

5. Control de Accesos.

El objetivo del presente dominio es controlar el acceso por medio de un sistema de restricciones y excepciones a la información como base de todo sistema de seguridad informática.

Para impedir el acceso no autorizado a los sistemas de información se deberían implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información, y estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.

Los procedimientos comprenden todas las etapas del ciclo de vida de los accesos de los usuarios de todos los niveles, desde el registro inicial de nuevos

usuarios hasta la privación final de derechos de los usuarios que ya no requieren el acceso.

La cooperación de los usuarios es esencial para la eficacia de la seguridad, es necesario concientizar a los mismos acerca de sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular aquellos relacionados con el uso de contraseñas y la seguridad del equipamiento.

5.1. Requisitos de negocio para el control de accesos.

Se deberían controlar los accesos a la información, los recursos de tratamiento de la información y los procesos de negocio en base a las necesidades de seguridad y de negocio de la Organización.

Las regulaciones para el control de los accesos deberían considerar las políticas de distribución de la información y de autorizaciones.

Los propietarios de activos de información que son responsables ante la dirección de la protección "sus" activos deberían tener la capacidad de definir y/o aprobar las reglas de control de acceso y otros controles de seguridad. Asegúrese de que se les responsabiliza de incumplimientos, no conformidades y otros incidentes.

5.2. Gestión de acceso de usuario.

Se deberían establecer procedimientos formales para controlar la asignación de los permisos de acceso a los sistemas y servicios de información.

Los procedimientos deberían cubrir todas las etapas del ciclo de vida del acceso de los usuarios, desde del registro inicial de los nuevos usuarios hasta su baja cuando ya no sea necesario su acceso a los sistemas y servicios de información.

Se debería prestar especial atención, si fuera oportuno, a la necesidad de controlar la asignación de permisos de acceso con privilegios que se salten y anulen la eficacia de los controles del sistema.

5.3. Responsabilidades del usuario.

La cooperación de los usuarios autorizados es esencial para una seguridad efectiva.

Los usuarios deberían ser conscientes de sus responsabilidades en el mantenimiento de controles de acceso eficaces, en particular respecto al uso de contraseñas y seguridad en los equipos puestos a su disposición.

Se debería implantar una política para mantener mesas de escritorio y monitores libres de cualquier información con objeto de reducir el riesgo de accesos no autorizados o el deterioro de documentos, medios y recursos para el tratamiento de la información.

Asegúrese de que se establecen las responsabilidades de seguridad y que son entendidas por el personal afectado. Una buena estrategia es definir y documentar claramente las responsabilidades relativas a seguridad de la información en las descripciones o perfiles de los puestos de trabajo.

Son imprescindibles las revisiones periódicas para incluir cualquier cambio. Comunique regularmente a los empleados los perfiles de sus puestos (p. ej., en la revisión anual de objetivos), para recordarles sus responsabilidades y recoger cualquier cambio.

5.4. Control de acceso a sistemas y aplicaciones.

Los medios deberían ser controlados y físicamente protegidos.

Se deberían establecer los procedimientos operativos adecuados para proteger los documentos, medios informáticos (discos, cintas, etc.), datos de entrada o salida y documentación del sistema contra la divulgación, modificación, retirada o destrucción de activos no autorizadas.

Asegure los soportes y la información en tránsito no solo físico sino electrónico (a través de las redes). Cifre todos los datos sensibles o valiosos antes de ser transportados.

6. Cifrado.

El objetivo del presente dominio es el uso de sistemas y técnicas criptográficas para la protección de la información en base al análisis de riesgo efectuado, con el fin de asegurar una adecuada protección de su confidencialidad e integridad.
La aplicación de medidas de cifrado se debería desarrollar en base a una política sobre el uso de controles criptográficos y al establecimiento de una gestión de las claves que sustenta la aplicación de las técnicas criptográficas.

6.1. Controles criptográficos.

Controles con el objetivo de proteger la confidencialidad, autenticidad o integridad de la información mediante la ayuda de técnicas criptográficas.
Las organizaciones deberían utilizarán controles criptográficos para la protección de claves de acceso a sistemas, datos y servicios, para la transmisión de información clasificada y/o para el resguardo de aquella información relevante en atención a los resultados de la evaluación de riesgos realizada por la organización.

Sería necesario el desarrollo adicional de procedimientos y asignación de funciones respecto de la administración de claves, de la recuperación de información cifrada en caso de pérdida, compromiso o daño de las claves y en cuanto al reemplazo de las claves de cifrado.

El uso de algoritmos de cifrado (simétricos y/o asimétricos) y las longitudes de clave deberían ser revisadas periódicamente para aplicar las actualizaciones necesarias en atención a la seguridad requerida y los avances en técnicas de descifrado.

Las firmas digitales proporcionan un medio de protección de la autenticidad e integridad de los documentos electrónicos y, en algunas ocasiones, podría ser necesario asesoramiento legal para establecer acuerdos especiales que respalden su uso.

7. Seguridad física y Ambiental.

El objetivo es minimizar los riesgos de daños e interferencias a la información y a las operaciones de la organización.

El establecimiento de perímetros de seguridad y áreas protegidas facilita la implementación de controles de protección de las instalaciones de procesamiento de información crítica o sensible de la organización, contra accesos físicos no autorizados.

El control de los factores ambientales de origen interno y/o externo permite garantizar el correcto funcionamiento de los equipos de procesamiento y minimizar las interrupciones de servicio.

La información almacenada en los sistemas de procesamiento y la documentación contenida en diferentes medios de almacenamiento, son susceptibles de ser recuperadas mientras no están siendo utilizados. Es por ello

que el transporte y la disposición final presentan riesgos que deben ser evaluados, especialmente en casos en los que el equipamiento perteneciente a la organización esté físicamente fuera del mismo (housing) o en equipamiento ajeno que albergue sistemas y/o preste servicios de procesamiento de información (hosting/cloud).

7.1. Áreas seguras.

Evitar el acceso físico no autorizado, daño e interferencia con la información y los locales de la organización.

Los medios de procesamiento de información crítica o confidencial deberían ubicarse en áreas seguras, protegidas por los perímetros de seguridad definidos, con las barreras de seguridad y controles de entrada apropiados.

Los medios de procesamiento deberían estar físicamente protegidos del acceso no autorizado, daño e interferencia.

El estándar parece centrarse, pero hay muchas otras áreas vulnerables a considerar, p. ej., armarios de cableado, "servidores departamentales" y archivos (recuerde: los estándares se refieren a asegurar la información, no sólo las TI). Algunas organizaciones usan tarjetas de identificación de colores para indicar las áreas accesibles por los visitantes.

Se debería asegurar la retirada de todos los pases de empleado y de visita cuando se vayan. Haga que los sistemas de acceso con tarjeta rechacen y alarmen ante intentos de acceso. Use pases de visita que se vuelvan opacos o muestren de alguna manera que ya no son válidos a las x horas de haberse emitido.

7.2. Seguridad de los equipos.

Deberían protegerse los equipos contra las amenazas físicas y ambientales. La protección del equipo es necesaria para reducir el riesgo de acceso no autorizado a la información y su protección contra pérdida o robo.

Así mismo, se debería considerar la ubicación y eliminación de los equipos. Se podrían requerir controles especiales para la protección contra amenazas físicas y para salvaguardar servicios de apoyo como energía eléctrica e infraestructura del cableado.

Haga que los vigilantes de seguridad o personal relevante impida a cualquiera (empleados, visitas, personas de soporte TI, mensajeros, personal de mudanzas, etc.) sacar equipos informáticos de las instalaciones sin autorización escrita.

Esté especialmente atento a puertas traseras, rampas de carga, salidas para fumadores, etc.

Tome en consideración el uso de lectura de códigos de barras para hacer los chequeos más eficientes.

8. Seguridad en la Operativa.

El objetivo es controlar la existencia de los procedimientos de operaciones y el desarrollo y mantenimiento de documentación actualizada relacionada.

Adicionalmente, se debería evaluar el posible impacto operativo de los cambios previstos a sistemas y equipamiento y verificar su correcta implementación, asignando las responsabilidades correspondientes y administrando los medios técnicos necesarios para permitir la segregación de los ambientes y responsabilidades en el procesamiento.

Con el fin de evitar potenciales amenazas a la seguridad del sistema o a los servicios del usuario, sería necesario monitorear las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad.

El control de la realización de las copias de resguardo de información, así como la prueba periódica de su restauración permite garantizar la restauración de las operaciones en los tiempos de recuperación establecidos y acotar el periodo máximo de pérdida de información asumible para cada organización.

Se deberían definir y documentar controles para la detección y prevención del acceso no autorizado, la protección contra software malicioso y para garantizar la seguridad de los datos y los servicios conectados a las redes de la organización.

Finalmente, se deberían verificar el cumplimiento de las normas, procedimientos y controles establecidos mediante auditorías técnicas y registros de actividad de los sistemas (logs) como base para la monitorización del estado del riesgo en los sistemas y descubrimiento de nuevos riesgos.

8.1. Responsabilidades y procedimientos de operación.

Asegurar la operación correcta y segura de los medios de procesamiento de la información mediante el desarrollo de los procedimientos de operación apropiados.

Se deberían establecer las responsabilidades y procedimientos para la gestión y operación de todos los medios de procesamiento de la información.

Se debería implantar la segregación de tareas, cuando sea adecuado, para reducir el riesgo de un mal uso del sistema deliberado o por negligencia.

8.2. Protección contra código malicioso.

El software y los medios de procesamiento de la información son vulnerables a la introducción de códigos maliciosos y se requiere tomar precauciones para evitar y detectar la introducción de códigos de programación maliciosos y códigos con capacidad de reproducción y distribución automática no autorizados para la protección de la integridad del software y de la información que sustentan.

El código malicioso es código informático que provoca infracciones de seguridad para dañar un sistema informático. El malware se refiere específicamente a software malicioso, pero el código malicioso incluye además scripts de sitios web (applets de Java, controles de ActiveX, contenido insertado, plug-ins, lenguajes de scripts u otros lenguajes de programación en páginas web y correo electrónico) que pueden aprovechar vulnerabilidades con el fin de descargar un malware.

El software y los recursos de tratamiento de información son vulnerables a la introducción de software malicioso como virus informáticos, gusanos de la red, caballos de troya y bombas lógicas.

Los usuarios deben estar al tanto de los peligros de los códigos maliciosos como el robo y destrucción de la información o daños e inutilización de los sistemas de la organización.

8.3. Copias de seguridad.

Mantener la integridad y la disponibilidad de los servicios de tratamiento de información y comunicación.

Se deberían establecer procedimientos rutinarios para conseguir la estrategia aceptada de respaldo para realizar copias de seguridad y probar su puntual recuperación.

Implante procedimientos de backup y recuperación que satisfagan no sólo requisitos contractuales sino también requisitos de negocio "internos" de la organización.

Básese en la evaluación de riesgos realizada para determinar cuáles son los activos de información más importantes y use esta información para crear su estrategia de backup y recuperación.
Hay que decidir y establecer el tipo de almacenamiento, soporte a utilizar, aplicación de backup, frecuencia de copia y prueba de soportes.

8.4. Registro de actividad y supervisión.

Los sistemas deberían ser monitoreados y los eventos de la seguridad de información registrados.

El registro de los operadores y el registro de fallas deberían ser usados para garantizar la identificación de los problemas del sistema de información.

La organización debería cumplir con todos los requerimientos legales aplicables para el monitoreo y el registro de actividades. El monitoreo del sistema debería ser utilizado para verificar la efectividad de los controles adoptados y para verificar la conformidad del modelo de política de acceso.

El viejo axioma del aseguramiento de la calidad "no puedes controlar lo que no puedes medir o monitorizar" es también válido para la seguridad de la información.

La necesidad de implantar procesos de supervisión es más evidente ahora que la medición de la eficacia de los controles se ha convertido en un requisito específico.

Analice la criticidad e importancia de los datos que va a monitorizar y cómo esto afecta a los objetivos globales de negocio de la organización en relación a la seguridad de la información.

8.5. Control del software en explotación.

Se trata de minimizar los riesgos de alteración de los sistemas de información mediante controles de implementación de cambios imponiendo el cumplimiento de procedimientos formales que garanticen que se cumplan los procedimientos de seguridad y control, respetando la división de funciones.

Verificar que los cambios sean gestionados por personal autorizado y en atención a los términos y condiciones que surjan de la licencia de uso.
Efectuar un análisis de riesgos previo a los cambios en atención al posible impacto por situaciones adversas.

Aplicar los cambios en sistemas de prueba y/o de manera escalonada empezando por los sistemas menos críticos además de aplicar medidas de backups y puntos de restauración junto a actividades adicionales que permitan retornar los sistemas al estado de estabilidad inicial con ciertas garantías.

Actualizar la documentación para cada cambio implementado, tanto de los manuales de usuario como de la documentación operativa.

Informar a las áreas usuarias antes de la implementación de un cambio que pueda afectar sus operaciones y envolver a usuarios finales en pruebas de aceptación del nuevo estado.

8.6. Gestión de la vulnerabilidad técnica.

Se trata de minimizar los riesgos de alteración de los sistemas de información mediante controles de implementación de cambios imponiendo el cumplimiento

de procedimientos formales que garanticen que se cumplan los procedimientos de seguridad y control, respetando la división de funciones.

Verificar que los cambios sean gestionados por personal autorizado y en atención a los términos y condiciones que surjan de la licencia de uso.

Efectuar un análisis de riesgos previo a los cambios en atención al posible impacto por situaciones adversas.

Aplicar los cambios en sistemas de prueba y/o de manera escalonada empezando por los sistemas menos críticos además de aplicar medidas de backups y puntos de restauración junto a actividades adicionales que permitan retornar los sistemas al estado de estabilidad inicial con ciertas garantías.

Actualizar la documentación para cada cambio implementado, tanto de los manuales de usuario como de la documentación operativa.

Informar a las áreas usuarias antes de la implementación de un cambio que pueda afectar sus operaciones y envolver a usuarios finales en pruebas de aceptación del nuevo estado.

Evite quedarse tan atrás en la rutina de actualización de versiones que sus sistemas queden fuera de soporte por el fabricante.

Pruebe y aplique los parches críticos, o tome otras medidas de protección, tan rápida y extensamente como sea posible, para vulnerabilidades de seguridad que afecten a sus sistemas y que estén siendo explotadas fuera activamente.

8.7. Consideraciones de las auditorías de los sistemas de información.

Maximizar la efectividad del proceso de auditoría de los sistemas de información y minimizar las intromisiones a/desde este proceso.

Durante las auditorías de los sistemas de información debieran existir controles para salvaguardar los sistemas operacionales y herramientas de auditoría.
Acordar con el/las áreas/s que corresponda los requerimientos de auditoría.

Limitar las verificaciones y/o tomar las medidas necesarias a efectos de aislar y contrarrestar los efectos de modificaciones realizadas al finalizar la auditoría (eliminar archivos transitorios, entidades ficticias y datos incorporados en archivos maestros; revertir transacciones; revocar privilegios otorgados).

Identificar claramente los recursos TI para llevar a cabo las verificaciones y puestos a disposición de los auditores (Sistemas de información, Bases de datos, hardware, software de auditoría, dispositivos magnéticos, personal, conexiones a red).

Documentar todos los procedimientos de auditoría, requerimientos y responsabilidades.

9. Seguridad en las Telecomunicaciones.

El objetivo es asegurar la protección de la información que se comunica por redes telemáticas y la protección de la infraestructura de soporte.

La gestión segura de las redes, la cual puede abarcar los límites organizacionales, requiere de la cuidadosa consideración del flujo de datos, implicaciones legales, monitoreo y protección.

La información confidencial que pasa a través de redes públicas suele requerir de controles adicionales de protección.

Los intercambios de información por parte de las organizaciones se deberían basar en una política formal de intercambio y en línea con los acuerdos de intercambio, y debiera cumplir con cualquier legislación relevante.

9.1. Gestión de la seguridad en las redes.

Se deberían controlar los accesos a servicios internos y externos conectados en red.

El acceso de los usuarios a redes y servicios en red no debería comprometer la seguridad de los servicios en red si se garantizan:

a) que existen interfaces adecuadas entre la red de la Organización y las redes públicas o privadas de otras organizaciones;
b) que los mecanismos de autenticación adecuados se aplican a los usuarios y equipos;
c) el cumplimiento del control de los accesos de los usuarios a los servicios de información.

Mantenga el equilibrio entre controles de seguridad perimetrales (LAN/WAN) e internos (LAN/LAN), frente a controles de seguridad en aplicaciones (defensa en profundidad).

Prepare e implante estándares, directrices y procedimientos de seguridad técnicos para redes y herramientas de seguridad de red como IDS/IPS (detección y prevención de intrusiones), gestión de vulnerabilidades, etc.

9.2. Intercambio de información con partes externas.

Se deberían realizar los intercambios sobre la base de una política formal de intercambio, según los acuerdos de intercambio y cumplir con la legislación correspondiente.

Se deberían establecer procedimientos y normas para proteger la información y los medios físicos que contienen información en tránsito.

Estudie canales de comunicaciones alternativos y "pre-autorizados", en especial direcciones de e-mail secundarias por si fallan las primarias o el servidor de correo, y comunicaciones offline por si caen las redes.
El verificar canales de comunicación alternativos reducirá el estrés en caso de un incidente real.

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

El objetivo es asegurar la inclusión de controles de seguridad y validación de datos en la adquisición y el desarrollo de los sistemas de información.

Definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan.

Definir los métodos de protección de la información crítica o sensible.

Aplica a todos los sistemas informáticos, tantos desarrollos propios o de terceros, y a todos los Sistemas Operativos y/o Software que integren cualquiera de los ambientes administrados por la organización en donde residan los desarrollos mencionados.

10.1. Requisitos de seguridad de los sistemas de información.

El diseño e implantación de los sistemas de información que sustentan los procesos de negocio pueden ser cruciales para la seguridad. Los requisitos de seguridad deberían ser identificados y consensuados previamente al desarrollo y/o implantación de los sistemas de información.

Todos los requisitos de seguridad deberían identificarse en la fase de recogida de requisitos de un proyecto y ser justificados, aceptados y documentados como parte del proceso completo para un sistema de información.

Se deberían considerar las implicaciones de seguridad asociadas con el uso de servicios de comercio electrónico, incluyendo transacciones en línea y los requisitos para los controles.

La integridad y disponibilidad de la información electrónica publicada a través de sistemas disponibles de publicidad deberían ser también consideradas.

Dentro de los sistemas de información se incluyen los sistemas operativos, infraestructuras, aplicaciones de negocio, aplicaciones estándar o de uso generalizado, servicios y aplicaciones desarrolladas por los usuarios.

10.2. Seguridad en los procesos de desarrollo y soporte

Se deberían controlar estrictamente los entornos de desarrollo de proyectos y de soporte.

Los directivos responsables de los sistemas de aplicaciones deberían ser también responsables de la seguridad del proyecto o del entorno de soporte. Ellos deberían garantizar que todas las propuestas de cambio en los sistemas son revisadas para verificar que no comprometen la seguridad del sistema o del entorno operativo.

Incorpore la seguridad de la información al ciclo de vida de desarrollo de sistemas en todas sus fases, desde la concepción hasta la desaparición de un sistema, por medio de la inclusión de "recordatorios" sobre seguridad en los procedimientos y métodos de desarrollo, operaciones y gestión de cambios.

10.3. Datos de prueba.

Se debería evitar la exposición de datos sensibles en entornos de prueba.

Para proteger los datos de prueba se deberían establecer normas y procedimientos que contemplen prohibir el uso de bases de datos operativas.

En caso contrario se deberían despersonalizar los datos antes de su uso y aplicar idénticos procedimientos de control de acceso que en la base de producción.

Procedimientos para la solicitud de autorización formal para realizar copias de la base operativa como base de prueba y de eliminación inmediata, una vez completadas las pruebas de la información operativa utilizada.

11. Relaciones con Suministradores.

El objetivo es implementar y mantener el nivel apropiado de seguridad de la información y la entrega de los servicios contratados en línea con los acuerdos de entrega de servicios de terceros.

La organización debe chequear la implementación de los acuerdos, monitorear su cumplimiento con los estándares y manejar los cambios para asegurar que los servicios sean entregados para satisfacer todos los requerimientos acordados con terceras personas.

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

La seguridad de la información de la organización y las instalaciones de procesamiento de la información no debería ser reducida por la introducción de un servicio o producto externo.

Debería controlarse el acceso de terceros a los dispositivos de tratamiento de información de la organización.

Cuando el negocio requiera dicho acceso de terceros, se debería realizar una evaluación del riesgo para determinar sus implicaciones sobre la seguridad y las medidas de control que requieren. Estas medidas de control deberían definirse y aceptarse en un contrato con la tercera parte.

Haga inventario de conexiones de red y flujos de información significativos con 3as partes, evalúe sus riesgos y revise los controles de seguridad de información existentes respecto a los requisitos.

Considere exigir certificados en ISO/IEC 27001 a los partners más críticos, tales como outsourcing de TI, proveedores de servicios de seguridad TI, etc.

11.2. Gestión de la prestación del servicio por suministradores.

La organización debería verificar la implementación de acuerdos, el monitoreo de su cumplimiento y gestión de los cambios con el fin de asegurar que los servicios que se ser prestan cumplen con todos los requerimientos acordados con los terceros.

¿Lo que recibe vale lo que paga por ello? Dé respuesta a esta pregunta y respáldela con hechos, estableciendo un sistema de supervisión de terceros proveedores de servicios y sus respectivas entregas de servicio.

Revise periódicamente los acuerdos de nivel de servicio (SLA) y compárelos con los registros de supervisión. En algunos casos puede funcionar un sistema de premio y castigo.

12. Gestión de Incidentes.

El objetivo es garantizar que los eventos de seguridad de la información y las debilidades asociados a los sistemas de información sean comunicados de forma tal que se apliquen las acciones correctivas en el tiempo oportuno.

Las organizaciones cuentan con innumerables activos de información, cada uno expuesto a sufrir incidentes de seguridad. Resulta necesario contar con una capacidad de gestión de dichos incidentes que permita comenzar por su detección, llevar a cabo su tratamiento y colaborar en la prevención de futuros incidentes similares.

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

Deberían establecerse las responsabilidades y procedimientos para manejar los eventos y debilidades en la seguridad de información de una manera efectiva y una vez que hayan sido comunicados.

Se debería aplicar un proceso de mejora continua en respuesta para monitorear, evaluar y gestionar en su totalidad los incidentes en la seguridad de información. Cuando se requieran evidencias, éstas deben ser recogidas para asegurar el cumplimiento de los requisitos legales.

Las revisiones post-incidentes y los casos de estudio para incidentes serios, tales como fraudes, ilustran los puntos débiles de control, identifican oportunidades de mejora y conforman por sí mismos un mecanismo eficaz de concienciación en seguridad.

Debería establecerse el informe formal de los eventos y de los procedimientos de escalado.

Todos los empleados, contratistas y terceros deberían estar al tanto de los procedimientos para informar de los diferentes tipos de eventos y debilidades que puedan tener impacto en la seguridad de los activos organizacionales.

Se les debería exigir que informen de cualquier evento o debilidad en la seguridad de información lo más rápido posible y al punto de contacto designado. Establezca y dé a conocer una hotline (generalmente, el helpdesk habitual de TI) para que la gente pueda informar de incidentes, eventos y problemas de seguridad.

13. Aspectos de la SI en la Gestión de la Continuidad de Negocio.

El objetivo es preservar la seguridad de la información durante las fases de activación, de desarrollo de procesos, procedimientos y planes para la continuidad de negocio y de vuelta a la normalidad.

Se debería integrar dentro de los procesos críticos de negocio, aquellos requisitos de gestión de la seguridad de la información con atención especial a la legislación, las operaciones, el personal, los materiales, el transporte, los servicios y las instalaciones adicionales, alternativos y/o que estén dispuestos de un modo distinto a la operativa habitual.

Se deberían analizar las consecuencias de los desastres, fallas de seguridad, pérdidas de servicio y la disponibilidad del servicio y desarrollar e implantar planes de contingencia para asegurar que los procesos del negocio se pueden restaurar en los plazos requeridos las operaciones esenciales, manteniendo las consideraciones en seguridad de la información utilizada en los planes de continuidad y función de los resultados del análisis de riesgos.

Deberían llevarse a cabo las pruebas pertinentes (tales como pruebas sobre el papel, simulacros, pruebas de failover, etc.) para (a) mantener los planes actualizados, (b) aumentar la confianza de la dirección en los planes y (c)

familiarizar a los empleados relevantes con sus funciones y responsabilidades bajo condiciones de desastre.

Minimizar los efectos de las posibles interrupciones de las actividades normales de la organización asociadas a desastres naturales, accidentes, fallas en el equipamiento, acciones deliberadas u otros hechos, protegiendo los procesos críticos mediante una combinación de controles preventivos y acciones de recuperación.

Instruir al personal involucrado en los procedimientos de reanudación y recuperación en relación a los objetivos del plan, los mecanismos de coordinación y comunicación entre equipos (personal involucrado), los procedimientos de divulgación en uso, los requisitos de la seguridad, los procesos específicos para el personal involucrado y responsabilidades individuales.

13.1. Continuidad de la seguridad de la información.

Se deberían determinar los requisitos de seguridad de la información al planificar la continuidad de los procesos de negocio y la recuperación ante desastres.
La organización debería establecer, documentar, implementar y mantener procesos, procedimientos y cambios de implementación para mantener los controles de seguridad de la información existentes durante una situación adversa.

Si los controles de seguridad no pueden continuar resguardando la información ante situaciones adversas, se deberían establecer, implementar y mantener otros controles para mantener un nivel aceptable de seguridad de la información.
Las organizaciones deberían verificar la validez y la efectividad de las medidas de continuidad de la seguridad de la información regularmente, especialmente cuando cambian los sistemas de información, los procesos, los procedimientos

y los controles de seguridad de la información, o los procesos y soluciones establecidas para la gestión de la continuidad de negocio.

13.2. Redundancias.

Se deberían considerar los componentes o arquitecturas redundantes cuando no se pueda garantizar el nivel de disponibilidad requerido por las actividades de la organización a través de arquitecturas sencillas típicas o los sistemas existentes se demuestren insuficientes.

Se deberían probar los sistemas de información redundantes para garantizar que la conmutación funcione adecuadamente.

14. Cumplimiento.

El diseño, operación, uso y administración de los sistemas de información están regulados por disposiciones legales y contractuales.

Los requisitos normativos y contractuales pertinentes a cada sistema de información deberían estar debidamente definidos y documentados.

El objetivo es cumplir con las disposiciones normativas y contractuales a fin de evitar sanciones administrativas a la organización y/o a los empleados que incurran en responsabilidad civil o penal como resultado de incumplimientos.

Se debe revisar la seguridad de los sistemas de información periódicamente a efectos de garantizar la adecuada aplicación de la política, normas y procedimientos de seguridad, sobre las plataformas tecnológicas y los sistemas de información.

14.1. Cumplimiento de los requisitos legales y contractuales

El diseño, operación, uso y gestión de los sistemas de información pueden ser objeto de requisitos estatutarios, reguladores y de seguridad contractuales.

Los requisitos legales específicos deberían ser advertidos por los asesores legales de la organización o por profesionales adecuadamente cualificados.

Los requisitos que marca la legislación cambian de un país a otro y pueden variar para la información que se genera en un país y se transmite a otro país distinto (por ej., flujos de datos entre fronteras).

Obtenga asesoramiento legal competente, especialmente si la organización opera o tiene clientes en múltiples jurisdicciones.

14.2. Revisiones de la seguridad de la información.

Se deberían realizar revisiones regulares de la seguridad de los sistemas de información.

Las revisiones se deberían realizar según las políticas de seguridad apropiadas y las plataformas técnicas y sistemas de información deberían ser auditados para el cumplimiento de los estándares adecuados de implantación de la seguridad y controles de seguridad documentados.

Alinee los procesos de auto-evaluación de controles de seguridad con el auto-evaluación de gobierno corporativo, cumplimiento legal y regulador, etc., complementados por revisiones de la dirección y verificaciones externas de buen funcionamiento.

Deberían existir controles para proteger los sistemas en activo y las herramientas de auditoría durante el desarrollo de las auditorías de los sistemas de información.

Invierta en auditoría TI cualificada que utilice ISO 27001, COBIT, ITIL, CMM y estándares y métodos de buenas prácticas similares como referencias de comparación.

Examine ISO 19011 "Directrices para la auditoría de los sistemas de gestión de la calidad y/o ambiental" como fuente valiosa para la realización de auditorías internas del SGSI [11].

Propuesta de Solución.

La Implantación de la norma ISO/IEC 27002:2013 para el Departamento Informático del Gobierno Autónomo Descentralizado Municipal del Cantón Salcedo, garantizara los controles internos y cumplimientos de los requisitos de gestión corporativa y de continuidad de la actividad dentro del mismo.

CAPITULO III

METODOLOGÍA

3.1 Modalidad básica de la investigación

La presente investigación se enmarcó dentro del paradigma crítico propositivo porque se realizó una investigación de todas las causas y factores del problema en el GAD municipal del Cantón Salcedo donde se pretende solucionar los problemas de seguridad de la información.

3.1.1 Investigación de campo

Se considera esta modalidad ya que el investigador acudió al lugar en donde se producen los hechos para obtener información relacionada con los objetivos del trabajo de grado. Las técnicas a ser utilizadas serán: entrevistas y la observación.

3.1.2 Investigación documental – bibliográfica

Se considera esta modalidad ya que se recurre a diferentes fuentes obtenidas de libros, artículos científicos, tesis desarrolladas en Universidades para profundizar enfoques con respecto al tema de la investigación.

Modalidad Aplicada

Por la utilización de los conocimientos adquiridos a lo largo de la carrera universitaria.

3.2 Población y Muestra

Población

DEPARTAMENTOS	POBLACIÓN
Departamento de sistemas	2
Departamento de registro a la propiedad	3
Departamento de agua Potable y Alcantarillado	2
Departamento de Obras Públicas	2
Departamento de Fiscalización	4
Departamento de Gestión Ambiental	2
Departamento Financiero	2
Departamento de Jefatura de Rentas	2
Departamento de Talento Humano	2
Departamento de Avalúos y Catastro	2
Departamento de Procuraduría Sindica	2
Departamento Administrativo	2
Departamento de Seguridad Ciudadana	2
Departamento de Contabilidad	2
Departamento de Recaudación y Tesorería	2
Departamento de Auditoria Interna	2
Departamento de Secretaria General	6
Departamento de Obras Públicas	2
Departamento de Desarrollo Social	2
Alcaldía	2
TOTAL	**47**

Tabla Nª 1: Población

Elaborado por: Sandra Criollo

Muestra

La presente investigación no requiere de muestra ya que la población es menor a 100.

3.3 Recolección de información

Se recolectará la información realizando entrevistas al personal encargado del departamento informático y demás del GAD municipal del cantón Salcedo, así también se buscará en Internet información virtual utilizando documentos técnicos, tesis, libros, todo esto para alcanzar los objetivos planteados.
También se realizará la recolección de información mediante observación en el entorno de la institución.

3.4 Procesamiento y análisis de datos

Para el procesamiento de la información se realizaron las siguientes actividades:

Los datos se los recogerán y se seleccionarán de acuerdo al área donde se maneje información del GAD Municipal del Cantón Salcedo y se pasara a tabular para poder aplicar los dominios de la norma ISO.

Se realizarán tablas con datos demostrativos de información para procesarlos y cuantificarlos de acuerdo a los objetivos que permitirá la implantación de la norma ISO/IEC 27002:2013.

El procesamiento de datos se lo realizará utilizando una herramienta informática a fin de organizarlo a través de gráficos estadísticos en cuanto a criterio de los inconvenientes presentados en la seguridad de la información dentro del GAD Municipal del Cantón Salcedo.

3.5 Desarrollo del Proyecto.

1. Estudio de la de la situación actual del departamento informático y sus políticas.
2. Análisis de la norma ISO 27002/2013.
3. Aplicación de técnicas de recolección de información en el departamento de sistemas y tabular los resultados.
4. Verificación de aspectos organizativos de la seguridad de la información.
5. Identificación los recursos tecnológicos, aplicaciones y consumos de servicios.
6. Análisis de vulnerabilidades.
7. Realización de informes y soluciones prácticas orientas a resolver los problemas que ocasionan la vulnerabilidad de la información.
8. Verificación con los resultados obtenidos se puede cumplir con la seguridad de la información.
9. Implantación de la norma ISO/IEC 27002:2013 en el departamento informático del GAD municipal del Cantón Salcedo.

CAPITULO IV

DESARROLLO DE LA PROPUESTA

Se detalla a continuación el desarrollo de la propuesta tomando en cuenta las normas que se aplicará con la norma ISO.

4.1 Planteamiento de la entrevista y análisis de información.

4.1.1 Objetivo de la entrevista.

Obtener información a través de una entrevista permitirá analizar la seguridad de la información en el GAD Municipal del Cantón Salcedo, podremos conocer si la gestión que tienen cuenta con criterios, parámetros o acciones, que ayudan a la protección de la información dentro del Municipio.

4.1.2 Diseño de la entrevista.

La entrevista está diseñada para cubrir todas las inquietudes sobre la seguridad de la información dentro del Municipio, a continuación, se presenta el formato de las preguntas con el objetivo que se desea obtener.

4.1.3 Recolección de información mediante técnica de la entrevista.

La entrevista se realizó en el GAD Municipal del Cantón Salcedo específicamente en el departamento de sistemas informáticos.

Análisis de la situación actual del Departamento de Sistemas del GAD Municipal del Cantón Salcedo.

La entrevista realizada al director del departamento de Sistemas del GAD Municipal del Cantón Salcedo reflejo que en el mismo no se cuenta con políticas claramente definidas acerca de protección de la información, de la misma manera no se lleva un control de acceso a los diversos sistemas, servicios y plataformas que se maneja dentro de la institución.

GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN SALCEDO DEPARTAMENTO DE SISTEMAS

ENTREVISTA ISO/IEC 27002:2013

Políticas de seguridad de la información.

- ¿El Departamento de Sistemas cuentan con políticas de seguridad de la información?

  SI (X) NO ( )

- ¿Se realiza frecuentemente una revisión de las políticas para la seguridad de la información?

  SI (X) NO ( )

- ¿El personal del GAD Municipal del Cantón Salcedo tiene conocimiento sobre las políticas de seguridad de la información?

  SI ( ) NO (X)

  Análisis: La persona responsable del Departamento de Sistemas respondió que existen políticas establecidas en el departamento a su cargo, las mismas que

frecuentemente son revisadas por la persona encargada, el resto del personal del GAD Municipal no tiene conocimiento sobre políticas de seguridad.

Interpretación: El departamento de sistemas debería establecer de forma correcta las políticas de actuación y manifestarlas para el apoyo y compromiso a la seguridad de la información, publicando y manteniendo políticas de seguridad en el GAD Municipal del Cantón Salcedo incluso se debe tomar en cuenta una estructura de gestión para iniciar y controlar la implantación de la seguridad de la información en todos los departamentos que conforma el Municipio.

Aspectos organizativos de la seguridad de la información.

- ¿El GAD Municipal de Salcedo cuenta con sitios para actividades de seguridad de la información?

  SI ( ) NO (X)

- ¿En la institución se ha contratado personal con conocimientos en materia de seguridad de la información?

  SI ( ) NO (X)

- ¿Al realizar contratos o convenios de contratación pública con empresas externas se exige cláusulas de seguridad de la información?

  SI ( ) NO (X)

- ¿Se han asignado responsabilidades de políticas de seguridad de la información dentro del Departamento?

  SI (X) NO ( )

  Análisis: El Departamento de Sistemas del GAD Municipal ha asignado responsabilidades de políticas de seguridad de la información. Pero el

departamento no cuenta con personal que tengan un amplio conocimiento en materia de seguridad de la información razón por la cual al realizar contratos o convenios con empresas externas no se exige ningún tipo de cláusula de este tipo.

Interpretación: Dentro del GAD Municipal y particularmente dentro del Departamento de Sistemas, se requiere personal con los conocimientos sobre la seguridad de la información ya que este puede estar contrarrestando constantemente a posibles ataques o robo de información del GAD Municipal y el mismo podría analizar los contratos con empresas aledañas dando la opinión sobre cláusulas que puedan manejar ambas partes sobre la información que se presente en los acuerdos establecidos.

Seguridad ligada a los recursos humanos.

- ¿Se cuenta con alguna política en la que se establezca que, en caso de abandono del puesto de trabajo de algún empleado se devuelva el equipamiento, así como también se elimine completamente los derechos de acceso (Acceso a información confidencial, Acceso a sistema)?

SI (X) NO ( )

Análisis: Dentro del Departamento de Sistemas del GAD Municipal de Salcedo existe la norma de que en caso de abandono de puesto de trabajo de algún empleado el mismo deberá devolver el equipamiento y el encargado eliminará los derechos de acceso del empleado.

Interpretación: Existe la responsabilidad con respecto a la protección de la información para cuando un empleado culmine su contrato con el GAD Municipal del Cantón Salcedo para oficializar su salida entregando cualquier documento que lo involucre con el mismo y quitándole el acceso al sistema donde este obteniendo información del mismo para evitar fuga de información.

Gestión de Activos

- ¿Se dispone de inventario de activos asociados a los recursos del tratamiento de la información tales como: recursos de información (bases de datos, documentación de sistemas, manuales de usuario), recursos de software (software de aplicaciones, sistemas operativos, herramientas de desarrollo, etc.), activos físicos (equipamiento informático, dispositivos móviles, pen drives, mobiliario, etc.) y servicios (servicios informáticos y de comunicaciones, calefacción, iluminación, energía eléctrica, etc.)?

  SI (X) NO ( )

- ¿Se cuenta con un área o departamento específico que se dedique a organizar inventarios de activos asociados a los recursos del tratamiento de la información?

  SI (X) NO ( )

- ¿La información que se maneja en su departamento tiene algún tipo de clasificación dependiendo su valor, sea esta: ¿requisitos legales, sensibilidad o criticidad para la organización?

  SI ( ) NO (X)

- ¿Se ha establecido procedimientos para la gestión de los medios de almacenamiento removibles de acuerdo con el valor de la información?

  SI ( ) NO (X)

- ¿Se protege los medios que contienen información contra acceso no autorizado, mal uso o corrupción durante el transporte fuera de los límites físicos de la organización?

SI ( ) NO (X)

Análisis: El departamento de Sistemas tiene conocimiento sobre los activos de información con los que cuenta el GAD Municipal, así como también dispone de espacios específicos para esta actividad. No se realiza clasificación de la información (directrices, etiquetado y manipulación, manipulación) y manejo de los soportes de almacenamiento (gestión de soporte extraíbles, eliminación y soportes físicos en tránsito).

Interpretación: Se pueden verificar que existe inventarios de activos como recursos de información, recursos de software, activos fijos y servicios ya que el objetivo principal es que el GAD Municipal del Cantón salcedo tenga conocimientos sobre su gestión de activos para evitar una mala administración, necesariamente se debe clasificar de acuerdo a la sensibilidad y criticidad de la información que contienen o bien de acuerdo a la funcionalidad que cumplen para señalar cómo ha de ser tratada y protegida dicha información que maneje cada uno.

Si se cuenta con un área para organizar los inventarios activos asociados a los recursos del tratamiento de la información, pero no se maneja los diversos grados de sensibilidad y criticidad ya que estos podrían requerir niveles de protección adicionales o de un tratamiento especial se debe utilizar un esquema de clasificación de la información para definir el conjunto adecuado de niveles de protección y comunicar la necesidad de medidas especiales para el tratamiento.

Es por eso que puede haber fuga de información sin procedimientos para la gestión de los medios de almacenamientos removibles con información del GAD Municipal del Cantón Salcedo, incluso puede salir del área del mismo y podría filtrarse dicha información o ser clonada en cualquier ya que no se ha controlado esta manera de movimiento de la información dentro de los departamentos.

Control de Accesos

- ¿Para las aplicaciones del GAD Municipal del cantón Salcedo se tienen políticas de control de acceso?

  SI (X) NO ( )

- ¿Las políticas de acceso son aplicadas?

  SI (X) NO ( )

- ¿Existe un control de acceso de usuarios en donde se mantiene restringido y controlado los privilegios de cada uno?

  SI (X) NO ( )

- ¿Se restringe el acceso de los usuarios y el personal de mantenimiento a la información y funciones de los sistemas de aplicaciones, en relación a la política de control de accesos definida? (si existiera).

  SI (X) NO ( )

- ¿Se cuenta con algún sistema de gestión de contraseñas que asegure contraseñas de calidad?

  SI (X) NO ( )

- ¿Se controla el acceso al código fuente de las aplicaciones software?

  SI (X) NO ( )

Análisis: El departamento de Sistemas del GAD Municipal si dispone de requisitos para el control de accesos, la gestión de acceso de los usuarios, responsabilidad de los usuarios y el control de acceso a sistemas y aplicaciones.

Interpretación: Si existe el control respectivo para los usuarios de los diferentes departamentos del GAD del Cantón Salcedo para poder restringir ciertas áreas q no sean de su incumbencia ya que el empleado podría tener acceso a información restringida por algún jefe de otro departamento y podría a ver algún tipo de fuga masiva de información de la misma no pueden cambiar sus permisos establecidos ya que el departamento de sistema los tiene restringidos desde el servidor a cada uno, también se tiene un sistema de contraseñas seguras que pueden encriptarse dentro del servidor para algún posible ataque que se haga por algún usuario malicioso e inculpar a otro empleado.

Desde el departamento de sistemas se tiene restringido al código fuente de las aplicaciones que se han desarrollado dentro del GAD Municipal es por eso que se debe utilizar controles criptográficos para la protección de claves de acceso a sistemas, datos y servicios, para la transmisión de información clasificada para evitar un riesgo de modificaciones dentro de las aplicaciones que se manejan dentro y evitar algún tipo de fraude.

Cifrado

- ¿La organización cuenta con alguna política de uso de controles criptográficos?

SI ( ) NO (X)

Análisis: El departamento de Sistemas del GAD Municipal no dispone de políticas de uso de controles criptográficos.

Interpretación: El uso de contar con algún tipo de cifrado de datos es de gran importancia dentro de cualquier entidad pública o privada, para evitar algún tipo de acceso indebido a la información por parte de personas ajenas a ellas.

Seguridad Física y Ambiental

- ¿Se dispone de algún sistema de seguridad física contra desastres naturales, ataques maliciosos o accidentes en las oficinas, salas e instalaciones de la organización?

  SI (X) NO ( )

- ¿Se dispone de áreas o sitios seguros para el desarrollo de proyectos o actividades propias de la organización?

  SI ( ) NO (X)

- ¿Se realiza el control de puntos de acceso a la organización como las áreas de entrada y salida, parqueaderos, (entre otras) para evitar el ingreso de personas no autorizadas a las dependencias de las instalaciones de procesamiento de información?

  SI ( ) NO (X)

- ¿Se controla que los equipos, la información o el software se retiren del sitio después de la debida autorización?

  SI ( ) NO (X)

- ¿En caso de alguna falla en el cableado de datos se está preparado para su pronta corrección?

  SI (X) NO ( )

  Análisis: El departamento de Sistemas del GAD Municipal dispone de un sistema de seguridad física para contrarrestar desastres naturales, así como también están preparados para una pronta corrección en caso de alguna falla en

el cableado, pero no controla ni supervisa el mantenimiento de equipos y la salida de activos fuera de las dependencias del departamento.

Interpretación: Debido a los cambios climáticos que existe en la actualidad el GAD Municipal si cuenta con un sistema de seguridad física contra los desastres naturales o accidentes que ocurran en el departamento de Sistemas para permitir y garantizar el correcto funcionamiento de los equipos de procesamiento y minimizar las interrupciones de los servicios que presta el municipio.

No existe sitios seguros para el desarrollo de proyectos o actividades propias de la organización está expuesto a robo de propiedad intelectual debido a que se realizarían en diversos departamentos expuestos al público.

No se tiene control de acceso al GAD del Municipio del Cantón Salcedo a pesar de que es un ente público y las personas pueden ingresar libremente no existe algún tipo de control para poder ingresar a los diferentes departamentos ni seguridad de cámaras o de guardias que impidas la entrada a las oficinas ya que estas tienen información clasificada del municipio y las personas podría ingresar libremente de la misma manera se observó que hay acceso por parqueaderos a peatones hacia las instalaciones del municipio, también se pudo observar que entre los mismo empleados ingresan a otras oficinas y pueden tomar diferentes dispositivos de dicha oficina y trasladarlos sin permiso o autorización de movilizaciones de equipos esto puede ocasionar fuga de información e incluso perdidas de dispositivos importantes dentro del GAD Municipal.

Existe un plan de contingencia para alguna falla del cableado en los de departamento por parte de sistemas, pero al mismo tiempo se observó que existe fallas en la estructura de la red ya que los cables están a la deriva de las paredes, pisos y colgando de otro piso a otro y podría existir fallas en la trasmisión de información y perdida de la misma.

Seguridad en las Operaciones

- ¿Se documenta los procedimientos operativos y los mismos se deja a disposición de todos los usuarios que los necesiten?

  SI ( ) NO (X)
- ¿Se dispone controles para la detección, prevención y recuperación ante afectaciones de malware en combinación con la concientización adecuada de los usuarios?

  SI (X) NO ( )
- ¿Existe una política de obtener copias de seguridad de la información?

  SI (X) NO ( )

  En caso de ser positiva la respuesta: ¿Con que frecuencia se obtienen copias de seguridad?

  SEMANALMENTE
- ¿Los sistemas están siendo monitoreados con frecuencia?

  SI (X) NO ( )
- ¿Se ha implementado procedimientos para controlar la instalación de software en sistemas operacionales?

  SI ( ) NO (X)
- ¿Se dispone de la oportuna información sobre las vulnerabilidades técnicas de los sistemas de información?

  SI ( ) NO (X)
- ¿Se planifica las actividades de auditoria de los sistemas de información?

  SI ( ) NO (X)

  Análisis: El departamento de Sistemas del GAD Municipal dispone de controles de protección contra malware; registro de actividad y monitorización. No se realiza ningún control del software operativo; ni se ha establecido una coordinación de la auditoría de sistemas de información.

  Interpretación: No existe procedimientos operativos para disposición de información entre los usuarios de un departamento esto podría tener alguna

complejidad al momento de realizar trabajos grupales entre los miembros de la misma oficina que deben utilizar información relevante para poder realizar sus labores diarias el caso de que uno de ellos posea esta información y no la pueda o quiera compartir por una razón.

El departamento de Sistemas tiene políticas de copias de seguridad de la información que se maneja dentro de este departamento y lo hace semanalmente que será almacenado en sus servidores para futuras utilidades y evitar contratiempos en algún posible cambio que se realice en el mismo proyecto o labor que se esté realizando.

No se tiene procedimientos para controlar la instalación de software es un gran problema para el GAD Municipal ya que acá se puede instalar cualquier software sin conocer su gravedad ni su utilidad en los equipos de los departamentos a pesar que las normas son estrictas para los entes públicos como el software libre.

Seguridad en las Telecomunicaciones.

- ¿Se cuenta con acciones en las redes para proteger la información en sistemas, aplicaciones y servicios?

SI (X) NO ( )

¿Cuales?

FIREWALL, PROXY DE ACCESO A INTRANET, ANTIVIRUS DEDICADO.

- ¿Se tiene establecido procedimientos y normas para proteger la información y los medios físicos que contienen información en tránsito?

SI (X) NO ( )

- ¿Se protege la mensajería electrónica?

SI (X) NO ( )

- ¿Existen acuerdos de confidencialidad y secreto?

SI ( ) NO (X)

Análisis: El departamento de Sistemas del GAD Municipal realiza una gestión de la seguridad en las redes, dispone de firewall, proxy de acceso a intranet, antivirus dedicado para para proteger la información en sistemas, aplicaciones y servicios, los medios físicos que contienen información y la mensajería electrónica también está controlada.

Interpretación: La protección de la información en el sistema, aplicaciones y servicios que tienen los servidores del departamento de sistemas son: Firewall, Proxy, Antivirus dedicado solo aplicados en esta oficina ya que se manejan todos los servidores del GAD Municipal del Cantón Salcedo, la mensajería electrónica es protegida dentro del servidor de correos que se maneja en el departamento de sistemas.

Adquisición, desarrollo y mantenimiento de los sistemas de información.

- ¿Se tiene requisitos de seguridad de los sistemas de información?

SI ( ) NO (X)

- ¿Existen procedimientos de control de los cambios que se realicen en los sistemas?

SI (X) NO ( )

- ¿Se hace uso de principios de ingeniería en protección de sistema para cualquier labor de implementación en los sistemas de información?

SI (X) NO ( )

- ¿Se supervisa y monitorea las actividades de desarrollo del sistema?

  SI (X) NO ( )

  Análisis: El departamento de Sistemas del GAD Municipal no cumple con requisitos de seguridad de los sistemas de información, en lo que tiene que ver al control y monitoreo que se realiza en los sistemas estos son supervisados por el departamento.

  Interpretación: Se hace uso de los principios de la ingeniera en protección de sistemas para la labor de implementación en los sistemas de información dando el ciclo de vida de desarrollo de sistemas en todas sus fases, desde la concepción hasta la desaparición de un sistema a través de la supervisión y monitoreo de sus actividades se realizaran en etapas establecidas. De la misma manera se realiza la respectiva supervisión a través del departamento de sistemas sobre los servicios que se contratan y que funcionan dentro del GAD Municipal del Cantón Salcedo como telefónica, acceso a internet entre otras.

  Relaciones con suministradores.

- ¿Se realiza una supervisión y revisión de los servicios prestados por terceros?

  SI (X) NO ( )

  Análisis: El departamento de Sistemas del GAD Municipal si realiza supervisión y revisión de los servicios prestados por terceros.

  Interpretación: El GAD Municipal del Cantón Salcedo realiza una correcta supervisión para asegurar que los servicios sean entregados para satisfacer todos los requerimientos acordados con terceras personas.

  Gestión de incidentes en la seguridad de la información.

- ¿Se ha documentado algunos de los puntos débiles de la seguridad de la información?

  SI ( ) NO (X)

- ¿Se realiza la valoración de eventos de seguridad de la información para poder tomar decisiones futuras?

  SI ( ) NO (X)

- ¿Se definen los procedimientos necesarios para la identificación, recopilación, adquisición y preservación de la información que puede servir de evidencia?

  SI ( ) NO (X)

  Análisis: El departamento de Sistemas del GAD Municipal no realiza gestión de las incidencias que afectan a la seguridad de la información con el objetivo de obtener mejoras.

  Interpretación: No se está documentando de vulnerabilidades que existan dentro del municipio eso llevaría a que si sigue ocurriendo se tendría q estar empezando a analizar por donde no exista seguridad de información, tampoco existe una valoración determinada para verificar el grado del daño que ocurra con los eventos de la seguridad de la información, no se tiene procedimientos para la identificación, recopilación, adquisición y preservación de la información que sirva de evidencia de haber existido fallas en la seguridad de la información.

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

- ¿Se cuenta con un plan de la continuidad de la seguridad de la información después de algún inconveniente?

  SI (X) NO ( )

- ¿Se realiza la verificación, revisión y evaluación de la continuidad de la seguridad de la información?

SI (X) NO ( )

- ¿Existe instalaciones aptas para el procesamiento de la información?

  SI (X) NO ( )

  Análisis: El departamento de Sistemas del GAD Municipal controla aspectos de Seguridad de la Información para la gestión de la continuidad de la organización así como la continuidad de la seguridad de la información.

  Interpretación: Existen instalaciones aptas para procesar la información dentro del departamento de sistemas donde se verifica y evalúa la seguridad de la información de los servicios que presta el GAD Municipal del Cantón Salcedo a través de sus funciones que presta a la comunidad.

  Cumplimiento.

- ¿Se cuenta con políticas de protección de datos y privacidad de la información personal?

  SI (X) NO ( )

  ¿Cuales?

  PLAN DE CONTINGENCIA

- ¿Los sistemas de información se revisan regularmente para verificar su cumplimiento con las políticas y normas de seguridad dispuestas por la información de la organización?

  SI (X) NO ( )

  Análisis: El departamento de Sistemas del GAD Municipal realiza regularmente revisiones del cumplimiento de las políticas de seguridad con las que cuenta la organización.

Interpretación: Existe protección de datos y privacidad de la información personal como el plan de contingencia que maneja, de existir algún evento inusual dentro del departamento de sistema se puede restablecer la información del usuario de manera rápida y segura, además se revisan regularmente los cumplimientos con las políticas y normas de seguridad que se establece en el GAD Municipal.

4.2 Planteamiento de la encuesta y análisis de información.

4.2.1 Objetivo de la encuesta.

Obtener información a través de una encuesta permitirá analizar la seguridad de la información en los departamentos del GAD Municipal del Cantón Salcedo, podremos conocer si la gestión que tienen cuenta con criterios, parámetros o acciones, que ayudan a la protección de la información dentro de cada departamento del Municipio.

4.2.2 Diseño de la encuesta.

La encuesta está diseñada para cubrir todas las inquietudes sobre la seguridad de la información dentro de los departamentos del Municipio, a continuación, se presenta el formato de las preguntas con el objetivo que se desea obtener.

4.1.3 Recolección de información mediante técnica de la encuesta.

La encuesta se realizó en el GAD Municipal del Cantón Salcedo en los siguientes departamentos:

Departamento de registro a la propiedad	Jefes y secretaria
Departamento de agua Potable y Alcantarillado	Jefe y secretaria
Departamento de Obras Públicas	Jefe y secretaria
Departamento de Fiscalización	Jefes y secretarias
Departamento de Gestión Ambiental	Jefe y secretaria

Departamento Financiero	Jefe y secretaria
Departamento de Jefatura de Rentas	Jefe y secretaria
Departamento de Talento Humano	Jefe y secretaria
Departamento de Avalúos y Catastro	Jefe y secretaria
Departamento de Procuraduría Sindica	Jefe y secretaria
Departamento Administrativo	Jefe y secretaria
Departamento de Seguridad Ciudadana	Jefe y secretaria
Departamento de Contabilidad	Jefe y secretaria
Departamento de Recaudación y Tesorería	Jefe y secretaria
Departamento de Auditoria Interna	Jefe y secretaria
Departamento de Secretaria General	Jefe y secretarias
Departamento de Obras Públicas	Jefe y secretaria
Departamento de Desarrollo Social	Jefe y secretaria
Alcaldía	Secretarias

ENCUESTA ISO/IEC 27002:2013

Políticas de Seguridad de la Información.

1. ¿Cuenta con políticas de seguridad de la información?

DETALLE	FRECUENCIA	PORCENTAJE
SI	2	4%
NO	43	96%
TOTAL	45	100%

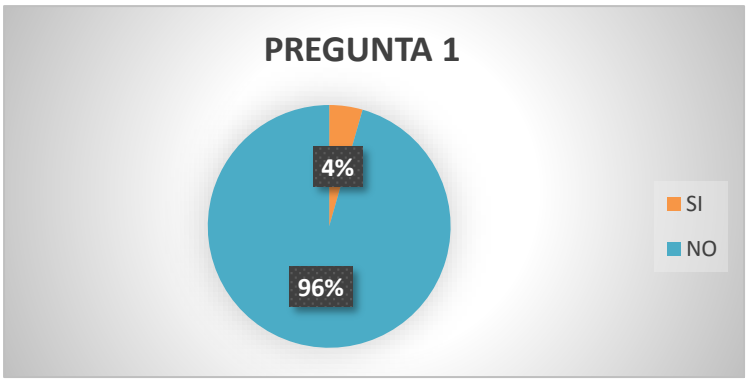


Gráfico 1

Análisis: De los 45 empleados encuestados de las áreas establecidas del GAD Municipal del Cantón Salcedo, 2 que corresponden al 4% manifiestan que si tienen políticas de seguridad de la información y 45 que corresponden al 96% indican que no tienen políticas de seguridad de la información en sus departamentos.

Interpretación: Los diferentes departamentos del GAD Municipal del Cantón Salcedo no cuentan con políticas de seguridad de la información, los resultados obtenidos en base en la encuesta realizada en cada oficina revelaron esto, de la misma manera no tienen políticas de seguridad para la información.

2. ¿El personal del GAD Municipal tiene conocimiento de las políticas de seguridad de la información?

DETALLE	FRECUENCIA	PORCENTAJE
SI	2	4%
NO	43	96%
TOTAL	45	100%

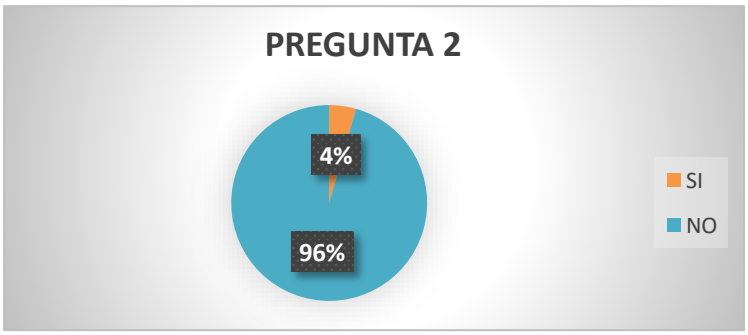


Gráfico 2

Análisis: De los 45 empleados encuestados de las áreas establecidas del GAD Municipal del Cantón Salcedo, 2 que corresponden al 4% manifiestan que tienen conocimientos de las políticas de seguridad de la información y 45 que corresponden al 96% indican que no cuentan con políticas de seguridad de la información.

Interpretación: Los diferentes departamentos del GAD Municipal del Cantón Salcedo no cuentan con políticas de seguridad de la información, los resultados obtenidos en base en la encuesta realizada en cada oficina revelaron esto, de la misma manera no tienen conocimiento de que son políticas de seguridad para la información haciendo que la información sea vulnerable en los departamentos.

Aspectos organizativos de la seguridad de la información.

3. ¿Se han asignado responsabilidades en políticas de seguridad de la información?

DETALLE	FRECUENCIA	PORCENTAJE
SI	2	4%
NO	43	96%
TOTAL	45	100%

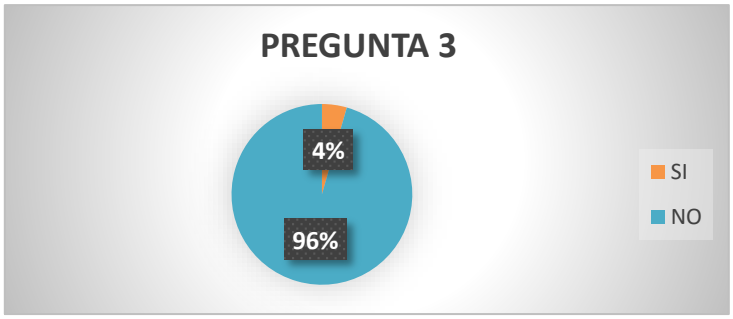


Gráfico 3

Análisis: De los 45 empleados encuestados de las áreas establecidas del GAD Municipal del Cantón Salcedo, un 96% no tiene responsabilidades ni cumple ningún rol para la seguridad de la información, mientras que el 4% podrían tener responsabilidades de seguridad de la información.

Interpretación: En aspectos organizativos de la seguridad de la información no se han asignado responsabilidades en las políticas para salvaguardar la información de los departamentos nuevamente quedaría expuesto la información de los departamentos del municipio ante alguna anomalía dentro de estos.

Gestión de Activos

4. ¿Se cuenta con políticas de seguridad que se encarguen de supervisar la manera en la que se manipula la información?

DETALLE	FRECUENCIA	PORCENTAJE
SI	0	0%
NO	45	100%
TOTAL	45	100%

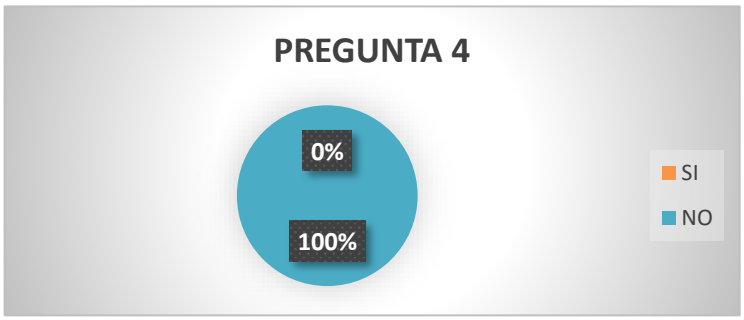


Gráfico 4

Análisis: De los 45 empleados encuestados de las áreas establecidas del GAD Municipal del Cantón Salcedo, 45 que corresponden al 100% manifiestan que no se supervisa la manipulación de la información.

Interpretación: Los diferentes departamentos del GAD Municipal del Cantón Salcedo no cuentan con supervisión de la manipulación de la información.

5. ¿Se ha establecido procedimientos para la gestión de los medios de almacenamiento removibles de acuerdo con el valor de la información?

DETALLE	FRECUENCIA	PORCENTAJE
SI	0	0%
NO	45	100%
TOTAL	45	100%

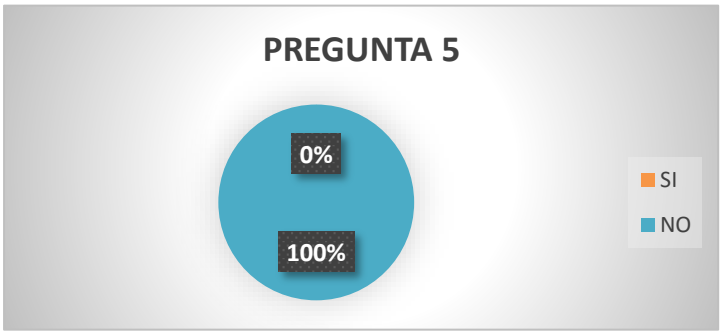


Gráfico 5

Análisis: De los 45 empleados encuestados de las áreas establecidas del GAD Municipal del Cantón Salcedo, 45 que corresponden al 100% manifiestan que no existe procedimientos para la gestión de los medios de almacenamientos.

Interpretación: Los diferentes departamentos del GAD Municipal del Cantón Salcedo no cuentan con procedimientos para la gestión de los medios de almacenamiento removibles.

6. ¿Se protege los medios que contienen información contra acceso no autorizado, mal uso o corrupción durante el transporte fuera de los límites físicos de la organización?

DETALLE	FRECUENCIA	PORCENTAJE
SI	0	0%
NO	45	100%
TOTAL	45	100%

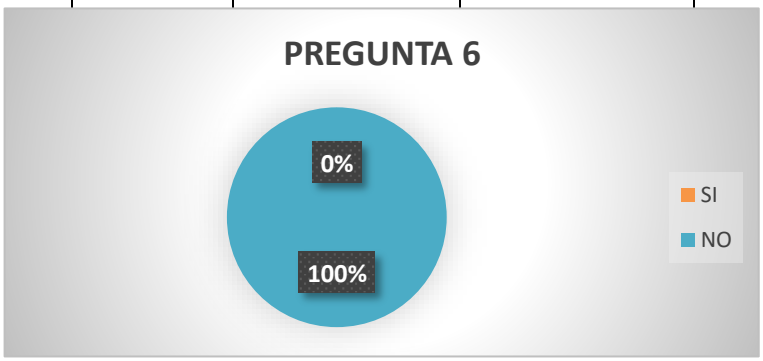


Gráfico 6

Análisis: De los 45 empleados encuestados de las áreas establecidas del GAD Municipal del Cantón Salcedo, 45 que corresponden al 100% manifiestan que no se protege los medios que contienen información contra acceso no autorizado.

Interpretación: Los diferentes departamentos del GAD Municipal del Cantón Salcedo no se protege los medios que contienen información contra acceso no autorizado.

7. ¿La información tiene algún tipo de clasificación dependiendo su valor, sea esta: requisitos legales, ¿sensibilidad o criticidad para la organización?

DETALLE	FRECUENCIA	PORCENTAJE
SI	0	0%
NO	45	100%
TOTAL	45	100%

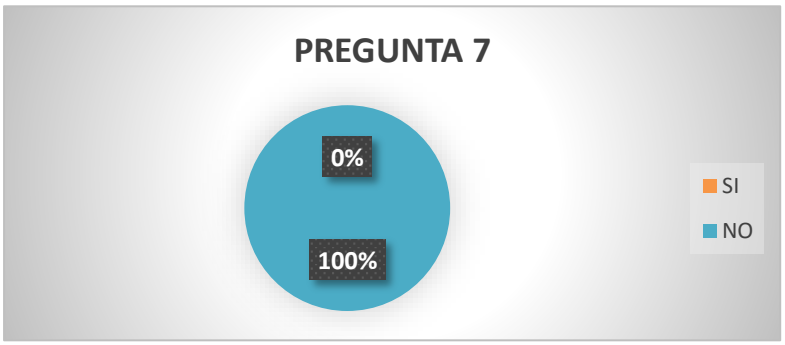


Gráfico 7

Análisis: En lo que se refiere al Dominio de Gestión de Activos un 100% de los servidores municipales no tienen conocimiento de los activos de información con los que cuenta cada uno de los departamentos. Y no existe una clasificación de la información en base a su valor.

Interpretación: No se cuenta con políticas de seguridad en la gestión de activos para supervisar la manipulación de la información cayendo en cuenta que puede ser manipulado por cualquier empleado información de los distintos

departamentos del GAD Municipal del Cantón Salcedo sin estar dentro de su área de trabajo.

En la protección de los medios que almacenan la información contra acceso no autorizado o mal uso durante el transporte fuera del GAD Municipal del Cantón Salcedo está inhabilitado y es por eso que, se debe asignar algún tipo de protección para evitar pérdidas de información o clonaciones de la misma para incurrir a la falsa transmisión de datos.

Seguridad en la Operativa

8. ¿Se dispone de controles para la detección, prevención y recuperación ante afectaciones de malware en combinación con la concientización adecuada de los usuarios?

DETALLE	FRECUENCIA	PORCENTAJE
SI	0	0%
NO	45	100%
TOTAL	45	100%

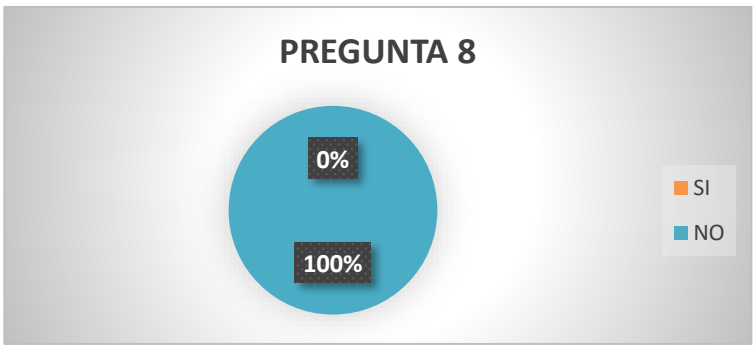


Gráfico 8

Análisis: Un 100% de los servidores municipales no dispone de controles para enfrentar algún tipo de ataque malicioso. La mayor parte de empleados de los departamentos no tienen conocimiento claro sobre el tema.

Interpretación: Se reporta que en los Departamentos del Municipio no se dispone de controles para la detección, prevención y recuperación ante afectaciones de malware en cuanto a los conocimientos que tenga los usuarios sobre la seguridad de la información.

Seguridad en las Telecomunicaciones.

9. ¿Se tiene establecido procedimientos y normas para proteger la información y los medios físicos que contienen información importante?

DETALLE	FRECUENCIA	PORCENTAJE
SI	4	9%
NO	41	91%
TOTAL	45	100%

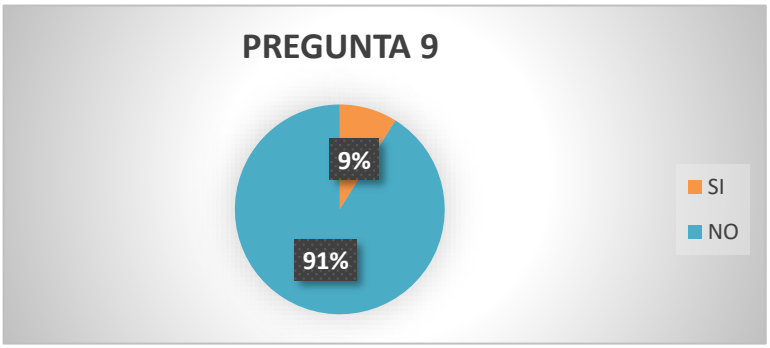


Gráfico 9

Análisis: De los 45 empleados encuestados de las áreas establecidas del GAD Municipal del Cantón Salcedo, 4 que corresponden al 9% manifiestan que si hay normas para proteger la información y los medios físicos de la información y 41 que corresponde al 91% que manifiestan lo contrario.

Interpretación: Los diferentes departamentos del GAD Municipal del Cantón Salcedo no se establecido procedimientos y normas para proteger la información y los medios físicos que contienen información

10. ¿Existen acuerdos de confidencialidad y secreto para la protección de información?

DETALLE	FRECUENCIA	PORCENTAJE
SI	4	9%
NO	41	91%
TOTAL	45	100%

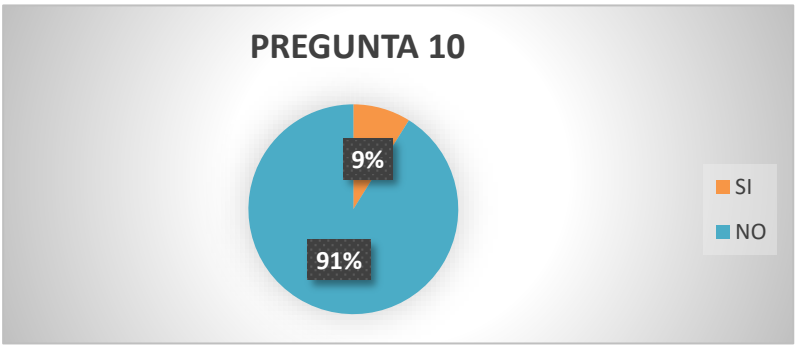


Gráfico 10

Análisis: En lo referente al Dominio de Seguridad en las Telecomunicaciones un 9% de los servidores municipales han establecido ciertas normas para protección de la información, mientras que el 91% simplemente segrega este tipo de actividades al Departamento de Sistemas.

Interpretación: Sobre la seguridad en las telecomunicaciones no se tiene establecido procedimientos y normas que protejan la información en medios físicos de almacenamiento que contenga la información del GAD Municipal de Cantón Salcedo, ya que puede ser extraviado o falsificada la información en transcurso de su movilización.

No existe la confidencialidad y secreto para la protección de la información dentro de los departamentos del GAD Municipal según la encuesta realizada a los trabajadores de las distintas oficinas a pesar de que se puede obtener

información dentro de la bodega que tienen algunos departamentos con información de los habitantes del Cantón e incluso del mismo Municipio pidiéndolo con una identificación para obtener dicha información a los bodegueros.

Conclusiones

- Con la información recolectada en los departamentos del GAD Municipal del Cantón Salcedo se puede concluir que se encuentra expuesta a ataques internos o externos. La falta de controles, políticas y conocimientos sobre la seguridad de la información en una institución la hace vulnerable a diversos ataques, por tal motivo se llegado a definir políticas de seguridad ya que estas serían la base para controlar y proteger los activos de la institución.

- El departamento de sistemas del GAD Municipal de Salcedo no cuenta con estándares de seguridad, para garantizar la confidencialidad, integridad y disponibilidad de los sistemas de información y comunicación.

- Dentro del GAD Municipal no existe una previa investigación de antecedentes del nuevo personal contratado, por lo que existe riesgos de fuga de información confidencial al no supervisar la correcta manipulación la misma.

- El departamento de sistemas no cuenta con personal cuya única responsabilidad sea los activos informáticos, así como la clasificación y manipulación de la información.

- La información procesada, en el GAD Municipal, así como servicios y sistemas esta expuestos a ataques informáticos.

- En el departamento de sistemas no existe una función o política que controle y administre los riesgos de la información.

- La información que es almacenada dentro de los diferentes departamentos del GAD Municipal del Cantón Salcedo, puede ser extraídos de manera fácil ya que no existe el control de movilización de información interna y externa.

Recomendaciones

- Es necesario definir controles y políticas para la seguridad de la información.

- Se recomienda designar responsables de gestión de las actividades relacionadas a los sistemas de información y comunicación para tener un control de las mismas.

- Se recomienda la implantación de la norma ISO/IEC 27002:2013 para mejorar la confidencialidad, integridad y disponibilidad de la información que sea procesada y utilizada dentro de los departamentos del GAD Municipal del Cantón Salcedo.

- Es recomendable realizar socializaciones acerca de la norma ISO/IEC 27002:2013, en el GAD Municipal del cantón Salcedo, con el fin de difundir los beneficios que estas proporcionan a las instituciones que las adoptan.

Análisis de vulnerabilidades y riesgos.

Para detectar vulnerabilidades dentro de la red del GAD Municipal del Cantón Salcedo, se utilizó la herramienta que permite escanear puertos abiertos *NMAP* que sirve para escaneo de puertos, protocolos entre otros, utilizado para resolver problemas detectados interna o externamente de una red.

Se realizó un escaneo de la intranet del GAD Municipal del Cantón Salcedo desde el departamento de sistemas el cual se obtuvo información de cuatro servidores que se encuentran en funcionamiento dentro del departamento, y se obtuvieron los siguientes resultados:

Servidor: 10.10.0.1

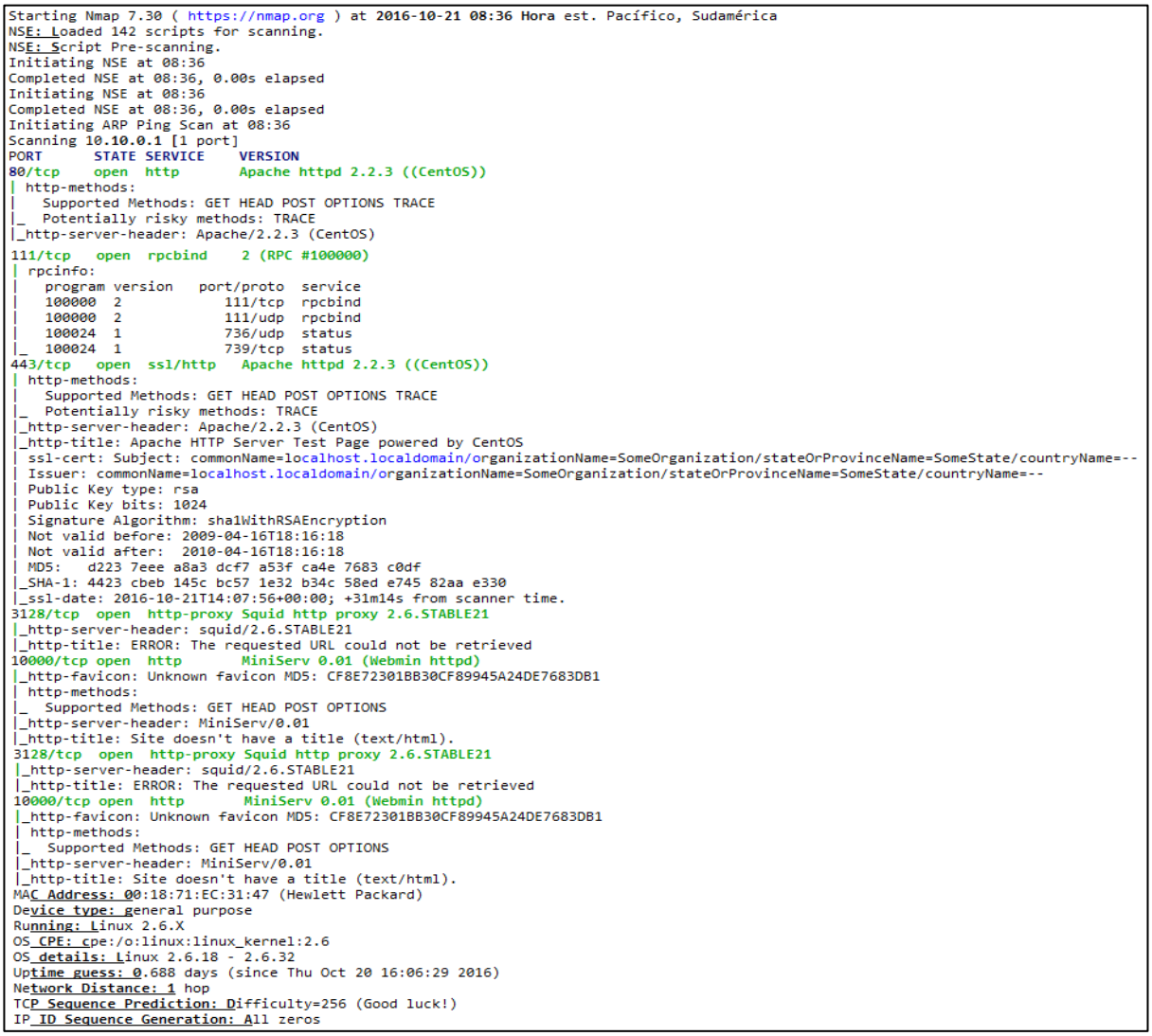


Gráfico Nº 1: Captura escaneo de puertos Servidor 10.10.0.1

Elaborado por: Sandra Criollo

Después de analizar el servidor 10.10.0.1, se pudo determinar lo siguiente:

- Puerto 80/TCP, donde se encuentra corriendo Apache httpd, ocupa un puerto por defecto y para el caso de HTTP puede permanecer abierto para comunicación entre equipos de la intranet, con el riesgo de encontrar vulnerabilidades dentro de la página que está alojado a través de ataques metasploid.

- Puerto 443/TCP, donde se encuentra un servidor CentOS de informes puede permanecer abierto para comunicación entre equipos de la intranet, pero se

puede ejecutar un exploit contra el servidor web vulnerable que este alojado en el mismo.

- Puerto 111/TCP, se encuentra corriendo el servicio RPCbind. Dicho servicio permite saber que otros servicios se encuentran corriendo en el servidor, el mismo que estando abierto podría ser objeto de utilización maliciosa para ataques DDoS es decir, denegación de servicios

- Puerto 3128/TCP, se encuentra corriendo un servidor proxy web con cache sirve para atender peticiones de otros ordenadores de la intranet puede permanecer abierto sin riesgo alguno.

- Puerto 1000/TCP, permite entrega de paquetes entre servidor y equipos de la intranet puede permanecer abierto sin riesgo alguno.

  Estos errores por parte de los encargados del servidor, puede ser una gran fuente de información en el momento de realizar un Test de Intrusión ya que se puede obtener no solo información acerca de la red interna, sino que además llegar a una carpeta de red y obtener los ficheros que se encuentren ahí.

Servidor 10.10.0.4

```
Starting Nmap 7.30 ( https://nmap.org ) at 2016-10-21 08:38 Hora est. Pacífico, Sudamérica
NSE: Loaded 142 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 08:39
Completed NSE at 08:39, 0.00s elapsed
Initiating NSE at 08:39
Completed NSE at 08:39, 0.00s elapsed
Initiating ARP Ping Scan at 08:39
Scanning 10.10.0.4 [1 port]
PORT      STATE SERVICE  VERSION
22/tcp    open  ssh      OpenSSH 4.3 (protocol 2.0)
| ssh-hostkey:
|   1024 4c:de:d6:3d:7c:e7:85:b1:77:bb:02:5f:76:2a:0f:67 (DSA)
|_  2048 fc:f6:ce:d1:a1:c8:ab:bd:c5:de:c4:b6:8a:bd:3e:51 (RSA)
53/tcp    open  domain   ISC BIND 9.3.6-P1
| dns-nsid:
|_  bind.version: 9.3.6-P1-RedHat-9.3.6-25.P1.el5_11.2
80/tcp    open  http     Apache httpd 2.2.22 ((EL))
|_http-generator: WordPress 3.6.1
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.2.22 (EL)
|_http-title: G.A.D. MUNICIPAL DEL CANTON SALCEDO
111/tcp   open  rpcbind  2 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2            111/tcp  rpcbind
|   100000  2            111/udp  rpcbind
|   100024  1            764/udp  status
|_  100024  1            767/tcp  status
443/tcp   open  ssl/http Apache httpd 2.2.22 ((EL))
| http-methods:
|   Supported Methods: GET HEAD POST OPTIONS TRACE
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.2.22 (EL)
|_http-title: Test Page for the Apache HTTP Server
| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName=SomeState/countryName=--
| Issuer: commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName=SomeState/countryName=--
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2011-08-29T15:44:25
| Not valid after:  2012-08-28T15:44:25
| MD5:   088d 31b3 ebe0 842f d731 f345 6646 444b
|_SHA-1: e10a b3a9 2fd7 8772 b7a6 5fc4 9930 e673 30cc d7dc
|_ssl-date: 2016-10-21T13:53:43+00:00; +14m02s from scanner time.
```

Gráfico Nº 2: Captura escaneo de puertos Servidor 10.10.0.4

Elaborado por: Sandra Criollo

Servidor 10.10.0.4, de los puertos abiertos escaneados se pudo determinar lo siguiente:

- Puerto 22 que aloja el servicio SSH que es un protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor y que permite a los usuarios conectarse a un host remotamente.

- Puerto 53 permite que los mensajes DNS se envían desde clientes DNS a los servidores DNS o entre servidores DNS, puede generar riesgo ya que si no existe el control necesario se puede incluir un equipo no registrado en el servidor y puede ocurrir robo de información.

- Puerto 80/TCP, donde se encuentra corriendo Apache httpd, ocupa un puerto por default y para el caso de HTTP puede permanecer abierto para comunicación entre equipos de la intranet, con el riesgo de encontrar vulnerabilidades dentro de la página que está alojado a través de ataques metasploid.

- Puerto 111/TCP, se encuentra corriendo el servicio RPCbind. Dicho servicio permite saber que otros servicios se encuentran corriendo en el servidor, el mismo que estando abierto podría ser objeto de utilización maliciosa para ataques DDoS es decir, denegación de servicios.

- Puerto 443/TCP, donde se encuentra un servidor CentOS de informes puede permanecer abierto para comunicación entre equipos de la intranet, pero si se ejecuta un exploit contra el servidor web vulnerable que este alojado en el mismo.

  Al encontrar estas vulnerabilidades podemos provecharlas por ejemplo usando un ataque de fuerza bruta que es el método que permite determinar una contraseña probando todas las combinaciones posibles hasta dar con la correcta.

Servidor 10.10.0.2

Gráfico Nº 3: Captura escaneo de puertos Servidor 10.10.0.2

Elaborado por: Sandra Criollo

Servidor 10.10.0.2, se escanea e identifica puertos abiertos, los mismos que pueden ser violentados, utilizando herramientas adecuadas:

- Puerto 25 que aloja el servicio de correo electrónico smtp. Este servicio puede ser utilizado por hackers para intentar, mediante un ataque de diccionario, averiguar la contraseña de algún usuario. Normalmente el objetivo es poder

lanzar spam desde el servidor, pero en algunos casos quizá el objetivo principal podría ser el averiguar la contraseña de un usuario administrador lo cual implicaría problemas dentro de la institución.

- Los puertos de Windows server nos permiten solo observar los nombres de los dominios, versiones entre otros que no correrían riesgos ya que solo permite visualizar contenido antes mencionado y puede categorizarse como un defecto de las versiones del SO.

Servidor 10.10.0.6

```
Starting Nmap 7.30 ( https://nmap.org ) at 2016-10-21 08:48 Hora est. Pacífico, Sudamérica
NSE: Loaded 142 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 08:48
Completed NSE at 08:48, 0.00s elapsed
Initiating NSE at 08:48
Completed NSE at 08:48, 0.00s elapsed
Initiating ARP Ping Scan at 08:48
Scanning 10.10.0.6 [1 port]
PORT      STATE SERVICE  VERSION
22/tcp    open  ssh      OpenSSH 5.3 (protocol 2.0)
| ssh-hostkey:
|   1024 f3:00:08:73:ed:e8:b3:1f:61:55:70:c0:37:cf:43:82 (DSA)
|_  2048 da:1e:2a:2c:f9:ba:ee:b8:a5:c7:b3:02:e4:77:4a:ed (RSA)
25/tcp    open  smtp     Postfix smtpd
|_smtp-commands: correo.salcedo.gob.ec, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
| ssl-cert: Subject: commonName=correo.salcedo.gob.ec/organizationName=Zimbra Collaboration Server/stateOrProvinceName=N/A/countryName=US
| Issuer: commonName=correo.salcedo.gob.ec/organizationName=Zimbra Collaboration Server/stateOrProvinceName=N/A/countryName=US
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2013-05-23T15:39:26
| Not valid after:  2018-05-22T15:39:26
| MD5:   fa00 d6ab b061 776b b3fe 9a93 75a7 e42d
|_SHA-1: f3df fa81 1196 6a64 5a26 6b00 53e2 1ca1 a74a 9ebc
|_ssl-date: 2016-10-21T13:47:27+00:00; -1m27s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|_    SSL2_RC4_128_WITH_MD5
53/tcp    open  domain   ISC BIND 9.8.2rc1
| dns-nsid:
|_  bind.version: 9.8.2rc1-RedHat-9.8.2-0.17.rc1.el6_4.4
110/tcp   open  pop3     Zimbra pop3d
|_pop3-capabilities: TOP EXPIRE(31 USER) UIDL XOIP USER IMPLEMENTATION(ZimbraInc) SASL(X-ZIMBRA) STLS
| ssl-cert: Subject: commonName=correo.salcedo.gob.ec/organizationName=Zimbra Collaboration Server/stateOrProvinceName=N/A/countryName=US
| Issuer: commonName=correo.salcedo.gob.ec/organizationName=Zimbra Collaboration Server/stateOrProvinceName=N/A/countryName=US
| Public Key type: rsa
| Public Key bits: 1024
443/tcp   open  ssl/http Zimbra Collabration Suite httpd
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Zimbra Web Client Sign In
| ssl-cert: Subject: commonName=correo.salcedo.gob.ec/organizationName=Zimbra Collaboration Server/stateOrProvinceName=N/A/countryName=US
| Issuer: commonName=correo.salcedo.gob.ec/organizationName=Zimbra Collaboration Server/stateOrProvinceName=N/A/countryName=US
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2013-05-23T15:39:26
| Not valid after:  2018-05-22T15:39:26
| MD5:   fa00 d6ab b061 776b b3fe 9a93 75a7 e42d
|_SHA-1: f3df fa81 1196 6a64 5a26 6b00 53e2 1ca1 a74a 9ebc
|_ssl-date: 2016-10-21T13:47:27+00:00; -1m27s from scanner time.
465/tcp   open  ssl/smtp Postfix smtpd
|_smtp-commands: correo.salcedo.gob.ec, PIPELINING, SIZE 10240000, VRFY, ETRN, AUTH PLAIN LOGIN, AUTH=PLAIN LOGIN, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
| ssl-cert: Subject: commonName=correo.salcedo.gob.ec/organizationName=Zimbra Collaboration Server/stateOrProvinceName=N/A/countryName=US
| Issuer: commonName=correo.salcedo.gob.ec/organizationName=Zimbra Collaboration Server/stateOrProvinceName=N/A/countryName=US
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2013-05-23T15:39:26
| Not valid after:  2018-05-22T15:39:26
| MD5:   fa00 d6ab b061 776b b3fe 9a93 75a7 e42d
| SHA-1: f3df fa81 1196 6a64 5a26 6b00 53e2 1ca1 a74a 9ebc
```

Grafico Nº 4: Captura escaneo de puertos Servidor 10.10.0.6

Elaborado por: Sandra Criollo

En el servidor 10.10.0.6, se identificó:

- Puerto 22 que aloja el servicio SSH que es un protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor y que permite a los usuarios conectarse a un host remotamente.

- Puerto 25 que aloja el servicio de correo electrónico smtp. Este servicio puede ser utilizado por hackers para intentar, mediante un ataque de diccionario, averiguar la contraseña de algún usuario. Normalmente el objetivo es poder lanzar spam desde el servidor, pero en algunos casos quizá el objetivo principal podría ser el averiguar la contraseña de un usuario administrador lo cual implicaría problemas dentro de la institución.

- Puerto 53 permite que los mensajes DNS se envían desde clientes DNS a los servidores DNS o entre servidores DNS, puede generar riesgo ya que si no existe el control necesario se puede incluir un equipo no registrado en el servidor y puede ocurrir robo de información.

- Puerto 110 como es pop3, el servicio smtp, pop3 está diseñado para recibir correo, que en algunos casos no es para enviarlo, como ya se ha hecho un análisis anterior el riesgo que puede presentar este puerto es un ataque de fuerza bruta o la forma de recuperar una clave probando todas las combinaciones posibles hasta encontrar aquella que permite el acceso. Y de esta puede causar inconvenientes dentro de los servidores.

- Puerto 443/TCP, donde se encuentra un servidor CentOS de informes puede permanecer abierto para comunicación entre equipos de la intranet, pero si se ejecuta un exploit contra el servidor web vulnerable que este alojado en el mismo.

- Puerto 465/TCP, aloja el servicio de correo electrónico smtp. Este servicio puede ser utilizado por hackers para intentar, mediante un ataque de diccionario, averiguar la contraseña de algún usuario. Normalmente el objetivo es poder

lanzar spam desde el servidor, pero en algunos casos quizá el objetivo principal podría ser el averiguar la contraseña de un usuario administrador lo cual implicaría problemas dentro de la institución es la alternativa del puerto 25 ya que cumple la misma función.

Conclusiones del análisis realizado.

- Los puertos comprendidos entre el 0 y el 1023 son puertos reservados para usos específicos que se encuentran reglamentados, el sistema operativo los abre para permitir su empleo por diversas aplicaciones mediante los llamados protocolos, por ejemplo: HTTP, FTP, TELNET, IRC, POP3, etc.

- Luego de analizar cada uno de los servidores se puede obtener información de lo que se encuentra en ellos como programas, servicios de correo electrónico de autenticación, entre otros, que se maneja dentro de cada servidor además información de las versiones de los programas y lo principal los puertos donde se encuentran alojados los mismos.

- A través de estos puertos abiertos se podría ingresar a los servidores y realizar algún tipo de ataque, como MetaSploit el mismo que es una suite o conjunto de programas, diseñada para explotar las vulnerabilidades de los equipos.

- De la misma forma conociendo la dirección IP de la aplicación, con herramientas especializadas se puede realizar un ataque de denegación de servicio, ataque que consiste en imposibilitar el acceso a los servicios y recursos de una organización durante un período indefinido de tiempo.

IMPLEMENTACION DE LA NORMA ISO/EC 27002:2013 EN EL DEPARTAMENTO INFORMÁTICO GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN SALCEDO.

Garantía.

Se garantiza el cumplimiento establecido dentro del GAD Municipal del Cantón Salcedo tanto como los controles internos y la gestión que está vigente en los diferentes departamentos del mismo, y la continuidad de todas las actividades mientras se realiza los respectivos análisis, pruebas que se realizara de la Norma ISO/EC 27002:2013.

Ya que el resultado de lo planteado dará un efecto de satisfacción de los estándares que permitirá estimar, a través de los cambios y modificaciones introducidos en las actividades diarias, la magnitud de los inconvenientes que se han presentado en las actividades contemporáneas será corregidas y en alguno de los casos mejorar los controles utilizados en cada departamento.

El cumplimiento del deber de protección, el departamento de sistemas garantiza la seguridad de la información de todos los departamentos que prestan servicio en todos los aspectos relacionados con lo laboral.

Introducción.

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, 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 el GAD Municipal del Cantón Salcedo, 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.

Diagnóstico de la Situación Actual.

La justificación de motivos hasta la presente fecha en la cual se ha establecido con los respectivos análisis y estudios realizados dentro del GAD Municipal del Cantón Salcedo, debido a esto se puede determinar que no se ha establecido la norma ISO 27002:2013 para la información, por lo cual se propone las siguientes recomendaciones que permitirá gestionar de manera más óptima en el departamento de sistemas.

Estructura Orgánica del GAD Salcedo.

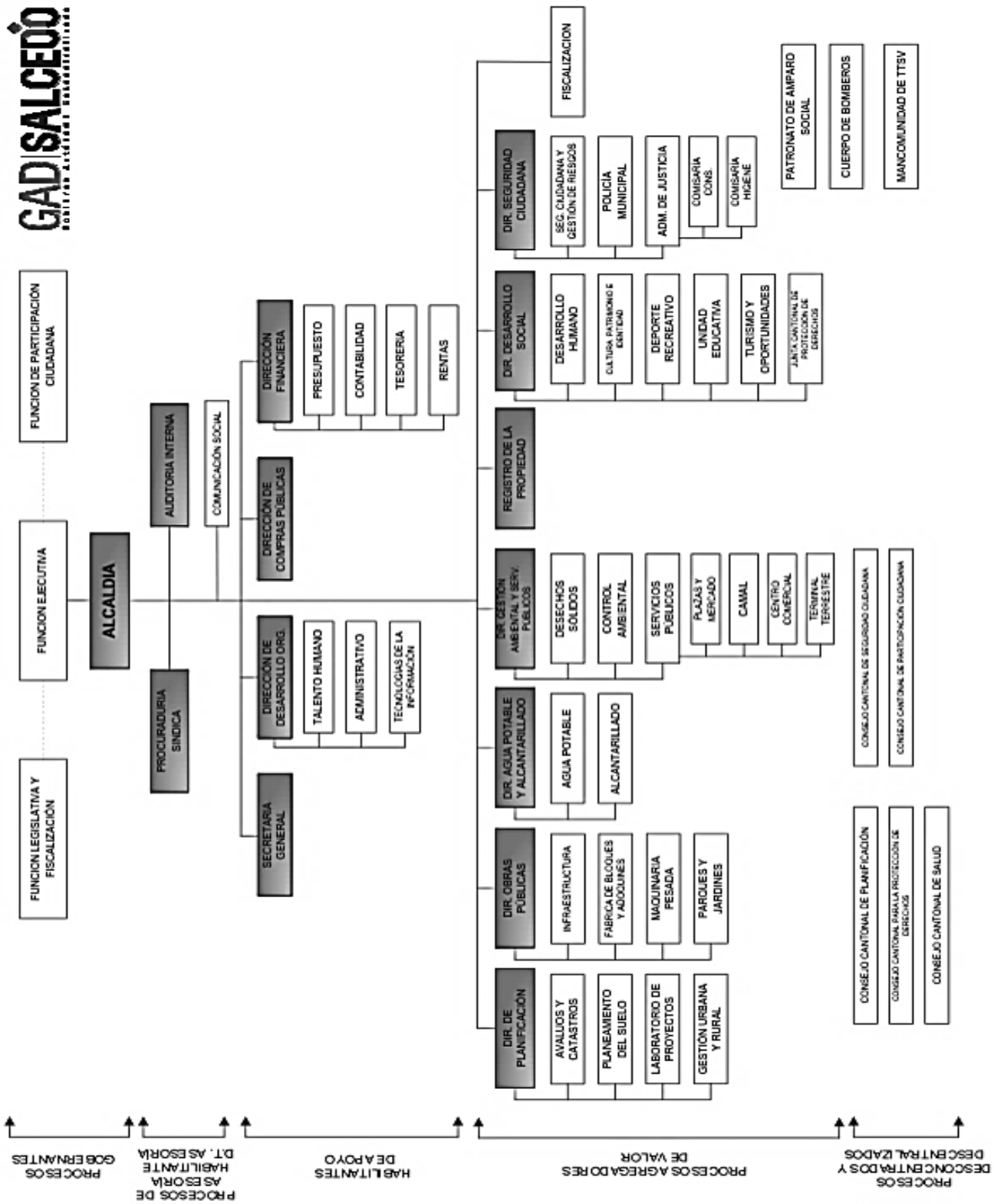


Gráfico Nº 5: Organigrama GAD Municipal del Cantón Salcedo

Elaborado por: el GAD Municipal

Objetivos Estratégicos.

Establecen intenciones más específicas dentro de cada punto, estos deben cubrir un período promedio de 4 años. Los objetivos estratégicos son declaraciones amplias orientadas a resultados, que delimitan las prioridades relativas de la organización y la estrategia general que se espera que ella siga.

Funciones del GAD Municipal del Cantón Salcedo.

1. Planificar, coordinar y ejecutar el ordenamiento territorial del Cantón, mediante la implementación de planes de construcción, mantenimiento, aseo, embellecimiento y reglamentación vial, de ornamentación y embellecimiento, de dotación de servicios públicos y de ordenamiento del tránsito y transporte terrestres.
2. Planificar, coordinar y ejecutar el desarrollo económico del Cantón, a través de planes de desarrollo turístico y el apoyo a micro organizaciones, pequeña industria e industria en actividades productivas.
3. Planificar, coordinar y ejecutar el desarrollo social, cultural y recreativo en coordinación con las organizaciones públicas o privadas del Cantón.
4. Planificar, coordinar y ejecutar el desarrollo ambiental del Cantón, armonizando el uso sostenible y sustentable de los recursos naturales a fin de contar con un ambiente sano y saludable.

Misión del GAD Municipal del Cantón Salcedo.

El GAD Municipal del Cantón Salcedo, es responsable de impulsar el buen vivir, a través del desarrollo territorial, económico, sociocultural y ambiental del cantón; a fin de que, Salcedo.

Visión del GAD Municipal del Cantón Salcedo.

El GAD Municipal de Salcedo fortalece su sistema de gestión organizacional, a fin de que éste sea artífice del desarrollo cantonal, de la participación ciudadana y del uso sostenible y sustentable de sus recursos.

LA NORMA ISO/IEC 27002:2013 PARA EL GAD MUNICIPAL DEL CANTÓN SALCEDO.

1. POLÍTICAS DE SEGURIDAD.

Objetivo: establecer los lineamientos iniciales para las políticas de seguridad de la información, las cuales garantizaran a preservar las tres principales características de la información como son integridad, confidencialidad y disponibilidad de la información. Las políticas establecidas se basan en los objetivos establecidos por la norma ISO [11].

1.1 Directrices de la dirección en seguridad de la información.

1.1.1 Conjunto de políticas para la seguridad de la información.

El departamento de sistemas del GAD Municipal del Cantón Salcedo dará seguimiento al cumplimiento de las normativas de la ISO para crear un ambiente de Seguridad de la Información los cuales tendrán las siguientes funciones:

- Velar por la seguridad de los activos informáticos.
- Gestión y Procesamiento de información.
- Elaboración de planes de seguridad.
- Capacitación a usuarios en temas de Seguridad.
- Gestionar y coordinar esfuerzos por crear un plan de contingencia, que de sustento o solución a problemas de seguridad dentro de la Institución. El mismo orientará y guiará a los empleados, la forma o métodos necesarios para salir adelante ante cualquier eventualidad que se presente.
- Informar sobre problemas de seguridad.
- Poner especial atención a los usuarios de la red institucional sobre sugerencias o quejas con respecto al funcionamiento de los activos de información.

El Departamento de Sistemas del GAD Municipal del Cantón Salcedo, a través de los encargados del departamento deberá elaborar manuales de roles, políticas y responsabilidades para cada uno de los trabajadores de cada departamento, el cual deberá estar documentado y aprobado por el alcalde del GAD Municipal del Cantón Salcedo, 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 del municipio Grafico [5].

- El jefe de cada Departamento dentro de la red institucional es el único responsable de las actividades precedentes a sus acciones.
- El Administrador de Sistemas es el encargado de mantener en buen estado los servidores dentro de la red institucional.
- Todo usuario de la red institucional gozara de absoluta privacidad sobre su información, o la información que provenga de sus acciones, salvo en casos en que se vea involucrado en actos ilícitos o contraproducentes para la seguridad de la red institucional.
- Los usuarios tendrán el acceso a Internet previa autorización siempre y cuando se cumplan los requisitos mínimos de seguridad para acceder a este servicio y se acaten las disposiciones de conectividad de la unidad informática.
- Las actividades administrativas tienen la primera prioridad por lo que a cualquier usuario utilizando otro servicio (por ejemplo: juegos, chat), sin estos fines, se le podrá solicitar salir o desconectar automáticamente los servicios si, así fuera necesario.

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

- Las revisiones de las políticas de seguridad se realizarán periódicamente, por los encargados del departamento de Sistemas.
- El departamento de sistema del GAD Municipal del Cantón Salcedo serán los encargados de la revisión de manuales y documentos que se realizaren sobre políticas de seguridad de la información.

2. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN.

Objetivo: Establecer la gestión que permita realizar tareas como la aprobación, implementación y asignación de procedimientos y responsabilidades de políticas de seguridad y garantizar la seguridad de la información en el uso de recursos de informática móvil y teletrabajo [11].

2.1. Organización interna

2.1.1. Asignación de responsabilidades para la seguridad de la información.

Con el cumplimiento de este control el encargado del departamento de sistemas del GAD Municipal del Cantón Salcedo asignará a un compañero dentro del área que será responsable de elaborar manuales de políticas y procedimientos para el área de tecnologías de la información y comunicación.

- Los miembros del departamento de sistemas, así como también un comité de Seguridad integrado por: Gestor de Seguridad, Responsable de Activos, Departamento de Sistemas serán los encargados de generar planes de contingencia anti desastres, etc.

2.1.2. Segregación de tareas.

- El encargado del departamento de Sistemas del GAD Municipal del Cantón Salcedo, capacitará a los demás trabajadores del departamento asignado a su responsabilidad, en cuanto al uso de los sistemas de información.
- En caso de ocurrir algún problema interno el servidor público encargado del área deberá solucionarlo en el caso que sea extremo acudir con el encargado del departamento de sistemas.
- Si un incidente ocurre en relación con el control de acceso, protección contra amenazas externas y de medio ambiente que el encargado del departamento no

pueda solucionarlo deben notificar al encargado de Seguridad de la Información del GAD Municipal del Cantón Salcedo en el departamento de sistemas.

2.1.3. Contacto con las autoridades.

- Deberá existir una constante comunicación con el encargado del departamento de sistemas del GAD Municipal del Cantón Salcedo, para que en el caso de realizar alguna actualización en las políticas de uso de la información darle a conocer sobre el caso, o cualquier duda que se tenga.

2.1.4. Contacto con grupos de interés especial.

- El encargado del departamento de sistemas del GAD Municipal del Cantón Salcedo se mantendrá al tanto sobre el tema de la seguridad de la información, tomando información de foros o grupos de seguridad externos, de la información acerca de cambios o actualizaciones de las políticas a nivel general.

2.1.5. Seguridad de la información en la gestión de proyectos.

- Cuando se realice proyectos que sean desarrollados en los diferentes departamentos del GAD Municipal del Cantón Salcedo, sin importar la índole del proyecto, cada trabajo deberá ser informado al departamento de sistemas que determinara las políticas que se aplicaran en dicho proyecto. Esta decisión la tomara el encargado de dicho departamento asignado.

2.2. Dispositivos para movilidad y teletrabajo.

2.2.1. Política de uso de dispositivos para movilidad.

- La red de datos para dispositivos móviles será restringida por control de acceso por parte del departamento de sistemas del GAD Municipal del Cantón Salcedo, debido a que se debe proteger la red a la que se accede.

2.2.2. Teletrabajo.

- La modalidad de Teletrabajo no está disponible en el GAD Municipal del Cantón Salcedo.

3. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.

Objetivo: asegurar que los empleados, contratistas y usuarios de terceras partes entiendan sus responsabilidades y sean aptos para las funciones que desarrollen además de reducir el riesgo de robo, fraude y mal uso de las instalaciones y medios, también asegurarse de que los empleados y contratistas están en conocimiento y cumplen con sus responsabilidades en seguridad de la información [11].

3.1. Antes de la contratación.

3.1.1. Investigación de antecedentes.

- Se realizarán concursos de méritos que deberán ser aprobados.
- Se solicitará referencias personales, laborares, para asegurarse de no tener problemas de índole legal al momento de contratar nuevo personal.

3.1.2. Términos y condiciones de contratación.

- Luego de la selección del nuevo empleado para el GAD Municipal del Cantón Salcedo, existirá un contrato legalizado, el que incluirá cláusulas de confidencialidad, las que el nuevo empleado debe cumplir ya sea persona natural o jurídica.

- En el contrato se incluirá sobre la aceptación de los términos y condiciones, que le obligan al funcionario a declararse como responsable de dar cumplimento a

las políticas de seguridad que estén vigentes dentro del GAD Municipal del Cantón Salcedo.

En el ANEXO 1 se encuentra el formulario de “Acuerdo de Confidencialidad”.

3.2. Durante la contratación.

3.2.1. Responsabilidades de gestión.

- Sera obligatorio que los términos y condiciones resalten en el contrato, estableciendo las diversas responsabilidades del empleado en cuanto a la seguridad de la información donde va a laborar.
- Los Departamentos deberán estar informados sobre las responsabilidades de seguridad informática, además de sanciones por incumplimiento de las mismas.

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

- Se debe realizar capacitaciones y requerimientos de seguridad, al asignar responsabilidades a cada encargado de departamento en su área. El encargado de organizar este tipo de actividades será el departamento de sistema del GAD Municipal del Cantón Salcedo para difundir las políticas de seguridad.

- El departamento de sistemas tendrá la responsabilidad de proporcionar el material necesario para la actividad, este material debe ser actualizado cada cierto tiempo que se vea necesario para estar claro en relación con el tema y cambios que hayan surgido.

3.2.3. Proceso disciplinario.

- El proceso debe pronosticar una respuesta gradual, tomando en consideración la gravedad del acto, su impacto en el GAD Municipal del Cantón Salcedo, si el

trabajador fue capacitado correctamente, la sanción se tomará en cuenta según el acuerdo de confidencial firmado en el contrato.

- Si el acto realizado tiene un nivel de gravedad perjudicial para el Municipio, el proceso permitirá la terminación inmediata de los derechos de acceso y privilegios otorgados, o la separación inmediata del cargo empleado dentro del Municipio.

3.3. Cese o cambio de puesto de trabajo.

- El empleado debe presentar su renuncia de terminación de sus funciones con un tiempo de antelación determinado de 15 días.
- De la misma manera, el empleado saliente será el encargado de entregar los activos al nuevo trabajador a ocupar la vacante, esto incluye claves de acceso, documentación, herramientas de trabajo, equipos de cómputo, etc.

4. GESTIÓN DE ACTIVOS.

Objetivo: identificar los activos en la organización y definir las responsabilidades para garantizar una protección adecuada, además asegurar que se aplica un nivel de protección adecuado a la información y evitar la divulgación, modificación, retirada o destrucción de activos no autorizada almacenada en soportes de almacenamiento [11].

4.1. Responsabilidad sobre los activos.

4.1.1. Inventario de Activos.

- Cada departamento, tendrá un responsable por el o los activos de importancia para el departamento.

- El GAD Municipal del Cantón Salcedo tendrá identificado todos los activos de información, en relación con los sistemas de información que maneja el municipio, así como sus respectivas ubicaciones físicas de cada activo.

- El inventario permanentemente será actualizado, 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, la responsabilidad recaerá sobre el encargado del que las custodia.

4.1.2. Propiedad de los Activos.

- En cuanto a propiedad de activos, el punto es que toda la información que pertenezca al GAD Municipal del Cantón Salcedo está sujeta a revisiones periódicas por parte del departamento de sistemas encargada de la seguridad de la información.

4.1.3. Uso aceptable de los activos.

La política se rige en que los activos de información del GAD Municipal del Cantón Salcedo son de propiedad de la misma, por tal motivo debe ser utilizada únicamente para fines laborales.

Lineamientos de seguridad de la información:

- Los recursos de servicio internet, correo electrónico y sistemas de información, serán utilizados para fines laborales, y con el permiso respectivo del departamento de sistemas.

- Cada encargado de sus departamentos identificará la labor que realizará los empleados a su cargo concediendo el debido acceso a la información mediante una asignación de roles que va a desempeñar el trabajador.

- Se prohíbe la divulgación de la información almacenada, creada o transmitida por los sistemas de Información del GAD Municipal del Cantón Salcedo.

- Las aplicaciones, software y sistemas de información que se utiliza dentro del GAD municipal del Cantón Salcedo deberán estar con su respectiva licencia o lo

que es recomendable utilizar software libre, esto será instalado por el personal del departamento de sistemas.

- El Departamento de sistemas será el encargado de establecer las cuentas a los usuarios de todos los departamentos, incluyendo acceso al control de los servidores en el caso que se necesite la información, auditorias de base de datos, monitoreo de uso de los sistemas.

- No se permite la compartición de acceso entre usuarios e información confidencial a terceras personas o entidades externas, vía mensaje de texto, transferencias vía correo electrónico o almacenamiento físico.
- Los sistemas de información estarán sujetos a ser auditadas por personal del departamento de sistema las veces que sea necesario o estableciendo un determinado tiempo por el mismo encargado.

- El departamento de sistemas implementara controles de seguridad de la información como firewall, antivirus, DMZ, etc. para asegurar que la información almacenada se encuentre respaldada.

- El GAD Municipal del Cantón Salcedo podrá revocar los privilegios de uso de activos de la información, emisión de sanciones e incluso trámites legales al empleado que ponga en riesgo la integridad, confiabilidad y disponibilidad de la información del municipio.

- Se establecen restricciones de acceso a redes inalámbricas, de acuerdo con las necesidades de cada departamento dentro del GAD Municipal del Cantón Salcedo.

- 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.

4.1.4. Devolución de activos.

Con el cumplimiento de este control el encargado de los activos cumplirá los lineamientos siguientes:

- Si el empleado saliente trabajo con información sobre tecnología o de administración relacionadas con su labor dentro del GAD Municipal del Cantón salcedo deberá dejar en conocimiento a través de documentos al departamento donde laboro.

- Toda la información del GAD Municipal del Cantón Salcedo que este en el equipo informático del empleado será removida del mismo.

- Devolución de equipos en general.

En el ANEXO 2 se encuentra el formulario de “Inventario de Hardware y Software de los computadores”.

4.2. Clasificación de la información.

4.2.1. Directrices de clasificación.

Con el desempeño de este control se debe clasificar la confidencialidad, integridad y disponibilidad.

Confidencialidad:

- Acceso privado e interno.
- La divulgación de la información traería consecuencias significativas al Municipio.
- La información se considera estrictamente confidencial.
- La información no tendrá acceso al público.

Integridad:

- La información se podrá modificar y rectificada con facilidad.

- La información se podrá modificar y rectificar ocasionando pérdidas mínimas en el Municipio.
- La información se podrá modificar, pero será más complicada para corregirla y podría existir pérdidas para el Municipio.
- La información se podrá modificar, pero no podría ser corregida y existirán pérdidas importantes para el municipio.

Disponibilidad:

- La información no afectara las operaciones del Municipio.
- La información que no esté habilitada por un tiempo de 5 días, podría afectar las operaciones del Municipio.
- La información que no esté disponible por un día podría afectar severamente las operaciones del Municipio.
- La información que no esté disponible durante una hora puede afectar significativamente las operaciones del Municipio.

4.2.2. Etiquetado y manipulado de la información.

- Se tendrá que identificar la información y los activos, que serán manipulados de mejor manera evitando daños o perdidas de la información, se manejará a través de colores según el nivel de riesgo.

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

Tabla Nª 2: Nivel de riesgo

Elaborado por: Sandra Criollo

- Para definir los controles de seguridad que se debe dar a cada una se identificara la información con los colores respetivos.

4.2.3. Manipulación de activos.

- Los empleados deben tener los conocimientos de los niveles de riesgos para que puedan ser manipuladas sin ningún problema todo tipo de información en sus departamentos.

4.3. Manejo de los soportes de almacenamiento.

4.3.1. Gestión de soporte extraíbles.

- Los encargados de cada departamento del GAD Municipal del Cantón Salcedo, deberán controlar los dispositivos extraíbles que pertenezca a su área de trabajo, estos estarán destinados a los procesos que se ejecuten dentro del departamento o de la misma manera si son utilizados para almacenar la información únicamente en el área de trabajo.

4.3.2. Eliminación de soportes.

- Se eliminará los dispositivos de almacenamiento, todo tipo de copias y/o clonaciones de la información, esto lo deberá realizar el servidor público encargado de su departamento.

4.3.3. Soportes físicos en tránsito.

- La información almacenada en los dispositivos de extraíbles que salen fuera del área del Municipio, deberá ser encriptados para evitar plagio o copias no autorizadas dentro del departamento ya que puede ser información interna del municipio.

5. CONTROL DE ACCESO.

Objetivo: controlar los accesos a la información y las instalaciones utilizadas para su procesamiento y garantizar el acceso a los usuarios autorizados e impedir los

accesos no autorizados a los sistemas de información y servicios, además de hacer que los usuarios sean responsables de la protección de la información para su identificación e impedir el acceso no autorizado a la información mantenida por los sistemas y aplicaciones [11].

5.1. Requisitos de negocio para el control de acceso.

5.1.1. Política de control de acceso.

Se debe tomar en cuenta los siguientes lineamientos para controles de acceso individual o grupal:

- Realizar un cronograma sobre los privilegios concedidos a los usuarios de los departamentos del GAD Municipal del Cantón Salcedo.
- Procedimientos para revocación de privilegios.
- Identificar y definir niveles de acceso estándar para empleados con labores básicas dentro de su departamento.
- Definir los requerimientos de seguridad para las diversas aplicaciones y sistemas del GAD Municipal del Cantón Salcedo.
- Identificar la información que debe ser protegida y que se encuentre ligada a los sistemas de información.
- Para obtención de acceso se deberá realizar una solicitud por escrito de la parte del departamento adjuntando los datos del empleado, esta deberá ser aprobada por la autoridad competente para que el encargado del departamento de sistemas habilite al usuario.

En el ANEXO 3 se encuentra el formulario de “Solicitud de Acceso a Sistemas de Información”.

5.1.2. Control de acceso a las redes y servidores asociados.

- El encargado del departamento de sistemas otorgará el acceso necesario a los servidores y redes, a los departamentos o usuarios que necesiten la información

lo cual deberán ser solicitados por el servidor público encargado del departamento que lo requiera, cada red deberá estar debidamente identificada para el fácil acceso de los usuarios con los roles que se tenga establecidos.

5.2. Gestión de acceso de usuario.

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

Con el desempeño de este control para la cancelación y registro del usuario se realizará de manera individual dando de baja o el acceso a la información que utilizara en su área de trabajo, él encargado del departamento de sistemas será el responsable y tomara en cuenta los lineamientos siguientes:

- Identificar con el nombre al usuario que lo identificará de manera segura para el departamento en el que labore, el usuario y el nivel de acceso asignado al empleado le permitirá realizar sus labores dentro de su área de trabajo.
- Verificación de los usuarios que acceden a los servidores, sistemas de información y redes de datos, verificando que sean los autorizados por el departamento de sistemas ya que podría existir algún tipo de infiltración.
- En el caso que el empleado termine sus funciones laborales dentro del GAD Municipal del Cantón Salcedo deberá ser notificado de inmediato al departamento de sistemas para darle de baja.

5.2.2. Gestión de los derechos de acceso asignados a usuarios.

- Se utilizará procedimientos para controlar los usuarios dentro del servidor que permitirán otorgar o quitar los permisos establecidos para las actividades que realizaran dentro de los diferentes departamentos.

5.2.3. Gestión de los derechos de acceso con privilegios especiales.

- Se utilizará las políticas de seguridad y privilegios otorgados para filtrar usuarios que necesiten permisos especiales dentro de los servidores o redes de

información siguiendo los requerimientos necesarios por parte del departamento de sistemas:

- Pasar un informe a cada departamento detallando sobre los privilegios de acceso para los servidores que deberán cumplir y de la misma manera para los sistemas de información y redes, etc.
- Asignar privilegios de acceso y modificación únicamente a los módulos que sean necesarios para el cumplimiento de las funciones del empleado.
- A través de herramientas se asignarán los privilegios a los empleados.
- Se deberá realizar revisiones continuas de todas las tareas que realice el empleado, que se encargará el departamento de sistemas.

5.2.4. Gestión de información confidencial de autenticación de usuarios.

Con el desempeño de este control al momento de otorgar una contraseña de acceso a los usuarios se cumplirá unos requerimientos necesarios para mejorar la dificultad de ataques maliciosos:

- Firmar un formulario de creación de usuario y responsabilidad de contraseñas.
- Se asignará una clave temporal al usuario de modo que el usuario sea quien cree la clave pasando a ser confidencial e intransferible, en el primer ingreso al sistema.
- Para la asignación de una clave a un usuario se debe tener la autorización del encargado del departamento donde va a laborar el mismo.
- El acceso de encriptación a los de servidores y sistemas se deben almacenar únicamente en el departamento de sistemas en lugares seguros de poco acceso al personal.
- El departamento de sistemas tendrá un listado de los servidores, usuarios y contraseñas para la administración de los mismos.

En el ANEXO 4 se encuentra el formulario de “Creación de usuario y responsabilidad de contraseñas”.

En el ANEXO 5 se encuentra el formulario de “Formulario de Listado de servidores y contraseñas”.

5.2.5. Revisión de los derechos de acceso de los usuarios.

Con la ejecución de este control se realizarán revisiones de los niveles de acceso que se le concedió a los usuarios de los departamentos del GAD Municipal del Cantón Salcedo tomando en cuenta los siguientes criterios:

- Los empleados que tenga permisos o privilegios especiales en su departamento deberán pasar por revisiones constantes especialmente si poseen acceso total de los sistemas del Municipio.
- El acceso de los encargados del departamento de sistemas y otros responsables de sus departamentos respectivos deberán pasar por revisión cada 3 meses.
- Para los usuarios en general se tendrá en cuenta cada mes la revisión respectiva o cada termino laborar de un empleado del Municipio.

5.2.6. Retirada o adaptación de los derechos de acceso.

- En el momento de que un servidor público termine sus funciones dentro del GAD Municipal del Cantón Salcedo se dará de baja todos los permisos y derechos concedidos al usuario en los sistemas y servicios del Municipio, por lo tanto, el encargado de cada departamento deberá notificar de manera inmediata la finalización del contrato del empleado para que el encargado de sistemas pueda tomar cartas en el asunto y eliminar el usuario del mismo.

5.3. Responsabilidad del usuario.

5.3.1. Uso de información confidencial para la autenticación.

Con el desempeño de este control los empleados de todos los departamentos deberán tener en cuenta los siguientes requerimientos para la seguridad de la información:

- El usuario deberá cambiar la clave provisionalmente otorgada por una personal al momento de ingresar por primera vez al sistema.
- Las claves de ingreso a los sistemas de información y servidores deberán ser confidenciales y por seguridad encriptadas en un formato más seguro para evitar robo de información.
- En el caso que un usuario olvide su contraseña deberá notificar de manera inmediata al departamento de sistemas del GAD Municipal del Cantón Salcedo.

5.4. Control de acceso a sistemas y aplicaciones

5.4.1. Restricciones de acceso a la información.

Con la realización de este control se tendrá que tomar en cuentas los siguientes requerimientos.

- El sistema deberá contener la página de inicio de login para que el usuario pueda colocar su id y contraseña respectiva e ingresar a sus funciones dentro del mismo, por lo tanto, el usuario tendrá limitada sus funciones dentro de la plataforma.
- El sistema debe permitir el acceso a la información autorizada y requerida, es decir se debe controlar los permisos de lectura, escritura y ejecución, para cada usuario.
- Se tomará en cuenta aplicar auditorías del sistema en cuanto a la información que maneja los usuarios verificando que sean las que debe manipular el mismo.

5.4.2. Procedimientos seguros de inicio de sesión.

- Los sistemas establecidos en cada departamento solo podrán tener acceso los usuarios registrados en las bases de datos que maneja el departamento de sistemas como seguridad de ingreso a la información del GAD Municipal del Cantón Salcedo permitiendo solamente el ingreso al usuario autorizado por dicho departamento.

5.4.3. Gestión de contraseñas de usuario.

- Las contraseñas que manejen cada usuario deberán tener un grado de complejidad para que no sean fácil de acceder a ellas y evitar un acceso no autorizado por parte del mismo, por lo tanto, las contraseñas deberán ser de un formato mínimo de 16 caracteres entre número, letras e incluso caracteres especiales.
- El usuario deberá estar consiente de los problemas de seguridad que acarrea la irresponsabilidad en la salvaguarda y uso de su contraseña.
- La práctica de guardar contraseñas en papel adherido al monitor o áreas cercanas al equipo de trabajo es una falta grave y sancionable.

5.4.4. Uso de herramientas de administración de sistemas.

- Los parámetros que tenga las aplicaciones que maneja el departamento de sistemas deberán tener restricción, solamente los encargados de los departamentos tendrían acceso total respectivo a su área de trabajo.
- Solo los encargados de los departamentos tendrían acceso para modificar acceso dentro de su área debido a las restricciones aplicadas a cada usuario.

5.4.5. Control de acceso al código fuente de los programas.

- Se restringirá el acceso al código fuente del sistema a los usuarios no a autorizados, para evitar alguna modificación o robo de información del sistema, en el caso que el desarrollador del sistema termine su contrato deberá dejar toda

información del sistema y se mantendrá suspendido su equipo de trabajo por el tiempo que no esté en su lugar de trabajo.

- Antes de ser puestas en ejecución las aplicaciones recibirán una auditoria sobre fallos o información errónea que puedan procesar.

6. CIFRADO.

Objetivo: garantizar un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información [11].

6.1. Controles criptográficos

6.1.1. Política de uso de controles criptográficos.

Con el cumplimiento de este control de seguridad de la información y su uso apropiado se deberán seguir los siguientes parámetros:

- El departamento de sistemas aplicara el mejor algoritmo de encriptación y tamaño de claves.
- Los controles criptográficos se utilizarán para la protección de claves de acceso a los servidores y sistemas de información de ser necesario.
- Los controles criptográficos se utilizarán, para la trasmisión información confidencial mediante el uso de redes de datos del departamento de sistemas.

6.1.2. Gestión de claves.

- El departamento de sistemas estipulará un tiempo para que las contraseñas puedan ser utilizadas dentro de los departamentos ejemplo: la contraseña tendrá una validez de 1 mes y deberá ser cambiada por otra no utilizada cada mes y así evitar clave clonadas o repetidas en el caso de haber dado la misma a otro usuario.

7. LA SEGURIDAD FÍSICA Y AMBIENTAL.

Objetivo: evitar el acceso físico no autorizado, los daños e interferencias a la información de la organización y las instalaciones de procesamiento de la información y evitar la pérdida, los daños, el robo o el compromiso de activos y la interrupción a las operaciones del GAD Municipal del Cantón Salcedo. [11].

7.1. Áreas seguras

7.1.1. Perímetro de seguridad física.

La restricción del acceso a recursos o activos de tecnología se tendrá en cuenta para la confidencialidad de la información del GAD Municipal de la Cantón Salcedo, por lo tanto:

- Se deberán tener controles biométricos en departamentos que tenga información importante para que puedan restringir esas áreas limitando el acceso a los usuarios que no requirieran esta información.

- Dentro del GAD municipal del Cantón Salcedo se deberá contar con cámaras de seguridad, vigilancia y alarmas para tener en cuenta quien ingresa al departamento y tener respaldos físicos en caso de alguna anomalía dentro del área.

7.1.2. Controles físicos de entrada.

- Se contará con un registro de cada persona que ingrese a un área determinada con los datos personales, cedula hora de ingreso y salida.

- Se deberán utilizar acceso biométrico, credenciales con foto actualizada, de esta manera se tendrá clasificada el ingreso a los departamentos de GAD Municipal del Cantón Salcedo el cual se deberá tener revisiones constantes para mantener actualizada la información de los usuarios.

7.1.3. Seguridad de oficinas, despachos y recursos.

Con la ejecución de este control se tendrá la seguridad de los departamentos en especial el departamento de sistema ya que en él se encuentra los servidores e información clasificada del GAD Municipal del Cantón Salcedo para ello se deberán aplicar los parámetros siguientes:

- Restringir acceso al personal no autorizado en los departamentos.
- Asegurar puertas y ventanas de los departamentos en caso de ser necesario se podría presentar un ingreso no autorizado fuera de horas de trabajo de terceras personas.
- Tener el equipamiento necesario dentro de cada departamento con las Tic´s necesarias.
- Respaldar la información en servidores y disco externos y evitar que tenga contacto con personal no autorizado.

7.1.4. Protección contra las amenazas externas y ambientales.

En el caso del GAD Municipal del Cantón Salcedo se debe atender los procesos de contabilidad, tesorería, administrativo-académicos, documentarios; que son las actividades que no podrían dejar de funcionar, por la importancia estratégica. La recuperación y puesta en marcha de los servidores que alojan dichos sistemas, es prioritario.

- Evitar que los suministros de papelería se encuentren al alcance de materiales inflamables.
- Tener un plan de contingencia en caso de una catástrofe natural de la misma manera contar con equipos contra incendios.
- Se deberá contar con un servidor especial de contingencia ubicado en otro sector para tener respaldos necesarios.
- Tramitar la garantía de los equipos dañados o comprar los equipos indispensables para la continuidad de las operaciones. Responsable encargado de Soporte y Mantenimiento.

- Se recoge los respaldos de datos, programas, manuales y claves. Responsable encargado de Redes.
- Revisar y probar la integridad de los datos. Responsable encargado de Desarrollo.

7.1.5. El trabajo en áreas seguras.

Con la realización de este control se aplicarán los siguientes procesos para ser aplicado internamente y externamente del GAD Municipal del Cantón Salcedo:

- Para el área restringida solo los usuarios que laboren dentro de él tendrán acceso concedido y la ubicación del lugar.
- El usuario externo tendrá limitaciones de existir el caso que sea requerido en esta área y tendrá que ser documentado su ingreso previo a una autorización otorgada por el encargado.
- No se podrá acceder con teléfonos móviles, equipo fotográfico dentro del área de la misma manera ingreso con bebidas y alimentos.

7.1.6. Áreas de acceso público, carga y descarga.

Con el cumplimiento de este control se cumplir con los siguientes parámetros:

- El personal que entrega los suministros no podrá acceder a áreas restringidas.
- Las áreas de carga y descarga deben estar alejadas del área de procesamiento de información.
- Mantener un listado de los suministros recibidos y ser revisados, para evitar algún material peligro y poder trasladar de manera segura la encomienda sin problemas al departamento destino.
- Auditoria de los suministros obtenidos y que sean los pedidos por los departamentos y se tenga constancia que son las requeridas.

7.2. Seguridad de los equipos

7.2.1. Emplazamiento y protección de equipos.

- Los equipos informáticos que tenga como objetivo el procesamiento de la información no se ubicarán en lugares que tenga acceso el público en general, estos deberán resguardados por cámaras y vigilancia autorizada y de limitado acceso de personas.

7.2.2. Instalaciones de suministro.

Con la realización de este control la energía eléctrica se deberá regular adecuadamente, para evitar bajas de electricidad o fallas en los sistemas, debido que ocurra algún inconveniente se deberá contar con equipos UPS que permitirán controlar los sistemas de manera segura en un tiempo limitado dependiendo de la característica del mismo que se encargara de proporcionar el cierre seguro de los sistemas cuando exista problemas de cortes de energía eléctrica.

7.2.3. Seguridad del cableado.

- El cableado de red interna de los departamentos contara con las categorías establecidas por el departamento de sistemas y estas deberán pasar por canaletas de plástico para evitar contacto con cables de electricidad que provocarían ruidos y cortes en la transmisión de los datos o paquetes, de la misma manera cada uno estará identificado hacia el patch panel de su departamento y por último se tendría un esquema graficado de cómo está estructurado la red del departamento de sistemas y de todo el GAD Municipal del Cantón Salcedo.

- Todos los equipos conectados en la red del GAD Municipal del Cantón Salcedo tendrá que seguir una auditoria para tener en cuenta que no tengan algún malware o gusano que pueda ser una amenaza para la información almacenada en los servidores.

7.2.4. Mantenimiento de los equipos.

Con la ejecución de este control se tendrá mantenimiento a las TIC´s que manejen información dentro del GAD Municipal del Cantón Salcedo según los parámetros establecidos:

- Siguiendo las recomendaciones de los mismos fabricantes de los equipos para obtener mejor resultados, solo los que se encuentren en el departamento sistemas laborando podrán realizar el mantenimiento asegurando lo realizado con un sello de garantía.
- Se realizará una auditoria del manteamiento dando a conocer los posibles daños o cambios realizados a las TIC's de piezas y posibles fallas de cada uno de ellos
- El personal de sistemas se les prohibirá la divulgación de la información almacenada en los equipos que pasen por sus manos al momento de realizarle el mantenimiento.

7.2.5. Salida de activos fuera de las dependencias del GAD Municipal del Cantón Salcedo.

- El equipo informático del GAD Municipal del Cantón Salcedo estará en su área establecido únicamente para cumplir con las labores del usuario.
- Si un equipo informático es necesitado fuera de su ubicación de trabajo se deberá pedir una autorización para poder trasladar el equipo, siempre tenerlo a la vista para que no ocurra nada durante su movilización.
- El equipo tendrá su encriptación respectiva para la información almacenada y en carpetas ocultas.

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

- Cuando se necesite realizar la movilización de los equipos se tendrá en cuenta el punto anterior de esta manera se podrá asegurar la disponibilidad, confidencialidad de la información del GAD municipal del Cantón Salcedo.

7.2.7. Reutilización o retirada segura de dispositivos de almacenamiento.

- Cuando se termine de utilizar un dispositivo de almacenamiento dentro de los departamentos, evitar que se contenga información del departamento de categoría sensible o licencias que puedan servir a futuro, por lo tanto, deberá pasar por el encargado del departamento para realizar una revisión esto servirá para que el dispositivo que contenga la información pueda ser reutilizado nuevamente.
- Bajo ninguna circunstancia se dejarán desatendidos los medios de almacenamiento, o copias de seguridad de los sistemas.
- La ubicación de los medios de almacenamiento deberá estar alejada de polvo, humedad, o cualquier contacto con material o químicos corrosibles.

7.2.8. Equipo informático de usuario desatendido.

- El encargado del departamento de sistemas realizara auditorias semestrales de los equipos y verificar que cada uno posea su contraseña respectiva, en el caso que el equipo se encuentre mal ubicado es decir en lugares húmedos se deberá realizar el cambio a un lugar seguro que no afecte al equipo.
- Del mismo modo el sistema deberá contar con su seguridad de antivirus al día.

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

- Se bloqueará el equipo informático cuando este en inactividad y volverá a requerir el usuario y contraseña del usuario el tiempo recomendado para inactividad seria de 10 min.

- El usuario deberá tener en cuenta que si sale de su lugar de trabajo donde se encuentra el equipo deberá bloquear el mismo para evitar que otros usuarios corrompan en su equipo.
- En los equipos de procesamiento de información solamente se utilizará medios de almacenamiento extraíbles que sean parten del GAD Municipal del Cantón Salcedo con previa revisión y autorización del departamento de sistemas para evitar fugas de información.

8. SEGURIDAD EN LA OPERATIVA.

Objetivo: Evitar el acceso físico no autorizado, los daños e interferencias a la información de la organización y las instalaciones de procesamiento de la información para garantizar que la información y las instalaciones de procesamiento de información estén protegidas contra el malware, además registrar los eventos relacionados con la seguridad de la información y generar evidencias y evitar la explotación de vulnerabilidades técnicas [11].

8.1. Responsabilidades y procedimientos de operación

8.1.1. Documentación de procedimientos de operación.

- Los procedimientos operativos, instalación, cambios en los servicios que presta el Municipio, procedimientos de reinicio de sistemas serán documentados para establecer la calidad y confianza de los servicios del GAD Municipal del Cantón Salcedo.
- El Monitoreo de los servidores que amacena la información, correos enviados y la información de errores o problemas operativos ubicados en el departamento de sistemas deberán ser documentados o archivados para tener un respaldo físico de cada trabajo información obtenida.

8.1.2. Gestión de cambios.

- Se evaluará las posibles implicaciones, estos cambios deben ser requeridos por los usuarios de la información, evaluados y aprobados por el encargado del departamento, los registros de cambios en la infraestructura, implicaciones, aprobación y planificación deberán ser documentadas.
- De la misma manera los cambios que sea realizados en la infraestructura del GAD Municipal del Cantón Salcedo deberán ser documentadas.

8.1.3. Gestión de capacidades.

- El departamento de sistemas monitoreara los sistemas y sus servicios que se operen dentro del GAD Municipal del Cantón Salcedo, teniendo en cuenta garantizar el rendimiento adecuado para futuros cambios que se podrían aplicar den estos.
- Analizar constantemente metodologías y tecnologías más óptimas para ser implementados en los sistemas y mejorarlos de una mejor forma.

8.1.4. Separación de entornos de desarrollo, prueba y producción.

- El entorno de ambiente para el desarrollo será en lugares de acceso restringido para evitar que el código fuente de los sistemas en proceso de desarrollo sean de libre acceso, de la misma manera los encargados de desarrollar las plataformas deberán documentar sus accesos en cada proyecto para evitar personas no autorizadas ingresen a los mismo y ocasionen perdidas de información.

8.2. Protección contra código malicioso.

- Los departamentos y usuarios no deben instalar software no autorizado por el departamento de sistemas, ya que este puede ser ilegal o el peor de los casos malicioso y podría causar inconvenientes en los equipos donde se realice la instalación incluso a los servidores del Municipio.

- Para evitar todo tipo de inconveniente con se deberá optar por la lista de software previamente identificado por el departamento de sistemas que se encargaría de revisar si contiene algún código malicioso.
- El departamento de sistemas es el encargado de realizar el monitoreo y actualización de los programas y los usuarios deberán reportar a este departamento sobre cualquier problema.
- El software que venga de empresas no reconocidas o acreditadas como no confiables, no tendrá ningún valor alguno para la Institución siempre que sea en formato ejecutable.

8.3. Copia de seguridad

8.3.1. Copias de seguridad de la información.

- Las copias de seguridad de la información y los respaldos deben estar correctas y sin errores, la cual se designará a un encargado del departamento de sistemas para llevar acabo la tarea.

  Para llevar acabo los respaldos de la información se lo realizara en un lugar adecuado y acondicionado tomando en cuenta los parámetros siguientes:

- Asignar un manual de procedimientos para definir el tipo de respaldo que se requiere para cada sistema y como volver a restaurarlos dependiendo del nivel de criticidad o confidencialidad de información que contenga tendrá su respectivo grado de encriptación.
- Los respaldos se obtendrán en dispositivos grandes de almacenamientos, ejemplo: Discos duros extraíbles, servidores, etc.

  Es por esto que se realizaran los Backups a los sistemas de información aplicado por una referencia:
- SIG-AME: Sistema integrado de administración financiera (Diario en el servidor).
- SIC: Sistema integral de catastros (Diario en el servidor).

- Sistemas desarrollados en el departamento de sistemas del GAD municipal del cantón salcedo.
- Sistema de control Biométrico de recursos humanos (cada 15 días en el computador del analista informático y cada mes a recursos humanos).
- Respaldo de información de movimiento entre los periodos que no se sacan backups es decir en días no laborales, feriados, etc.
- Uso obligatorio de un formulario de control de ejecución del programa de backups diarios, semanales y mensuales.
- Almacenamiento de los backups en condiciones ambientales optimas, dependiendo del medio de almacenamiento empleado.
- Almacenamiento de los backups en lugares diferentes donde reside la información primaria.

En el ANEXO 7 se encuentra el formulario de “registro de Backups”.

8.4. Registro de actividad y supervisión

8.4.1. Registro y gestión de eventos de actividad.

- Dentro de las bases de datos se crearán consultas que permita al usuario en el momento de crear, editar o eliminar se actualicen las auditorias automáticamente, estas deberán estar bien desarrolladas evitando fallas que puedan producirse en el sistema.

8.4.2. Protección de los registros de información.

- Los usuarios deben tener definidos sus actividades y los permisos otorgados para la manipulación de información y asignación de roles dependiendo de la labor del empleado, adicional el sistema deberá proporcionar el acceso a varios usuarios simultáneamente.

8.4.3. Registros de actividad del administrador y operador del sistema.

- Los encargados del departamento de sistema llevaran un registro de las actividades en donde reflejara la hora, la actividad realizada, usuarios y adicionales en caso de ser necesario es necesario que dentro de las bases de datos se agregue una tabla para los procedimientos de auditoria.

8.4.4. Sincronización de relojes.

- Es obligatorio tener un reloj principal 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.

8.5. Control del software en explotación

8.5.1. Instalación del software en sistemas en producción.

- Los usuarios involucrados serán notificados con anterioridad del cambio el mismo, y asegurar que el cambio no afecte las funcionalidades de los sistemas de información, es decir que para realizar un cambio en los equipos de los empleados o encargado por parte del departamento de sistema se deberá avisar con anticipación a los mismos para que estos puedan respaldar su información por seguridad.

8.6. Gestión de vulnerabilidad técnicas

8.6.1. Gestión de las vulnerabilidades técnicas.

- Se asignará un responsable en el departamento de sistemas que se encargará de monitorear y explorar vulnerabilidades que puedan transcurrir en los

departamentos del GAD Municipal del Cantón Salcedo, para poder evitar problemas en los equipos y sistemas instalados.

- En el momento que se detecte una vulnerabilidad se tomara acciones y se realizara un análisis para poder evitar que exista ese túnel de acceso, para esto se deberá actualizar parchar o configurar de mejor manera los servicios que presenten este inconveniente.

8.6.2. Restricciones en la instalación de software.

- Se permanecerá en constante observación monitoreo todas las TIC's del GAD Municipal del Cantón Salcedo desde el departamento de sistemas, también se verificará que los equipos cuenten con el sistema autorizado por el departamento incluso el software que deberán ocupar para su labor de trabajo, se manejara bloqueos de juegos o material inapropiado que distraiga al usuario.

8.7. Consideraciones de las auditorías de los sistemas de información.

8.7.1. Controles de auditoria de los sistemas de información.

Con el cumplimiento de este control punto de seguridad de la información se considera necesario la auditoria interna y externa para optimizar su funcionamiento.

Las auditorias deben tener los siguientes registros:

- Id de Usuario
- Hora y fecha de ingreso y salida
- Hora y fecha de actualización
- Dirección Ip
- Nombre del equipo donde se realizó la sesión
- Obtener un registro de accesos fallidos y de ingresos.
- Monitoreo de los accesos a utilidades, aplicaciones y departamentos.

- Protección de anti-malware, anti-virus y firewall.

9. SEGURIDAD EN LAS TELECOMUNICACIONES.

Objetivo: evitar el acceso físico no autorizado, los daños e interferencias a la información de la organización y las instalaciones de procesamiento de la información para garantizar y mantener la seguridad de la información que transfiere una organización internamente o con entidades externas [11].

9.1. Gestión de la seguridad en las redes

9.1.1 Controles de red.

Con el desempeño de este control el departamento de sistemas se encargará de monitorear las redes y administrarlas, garantizando que la información transmitida sea segura para los usuarios y evadir los accesos no permitidos.
Para ello debemos cumplir con los siguientes requerimientos:

- En el departamento de sistemas se establecerá las tareas de administración y monitoreo de redes, incluyendo a los equipos de comunicación.
- Asegurar la confidencialidad de la información transmitida por los servidores de red.
- Tener un registro de acceso a la red para controlar las actividades realizadas.
- Para los equipos de conectividad hay que cambiar las configuraciones por defecto. Además,
- Se deberá cerrar la sesión durante 30 segundos de inactividad.
- Guardar registros de auditoria.
- Sacar respaldos de configuración de los switchs y routers en el caso de ser inalámbricos que se utilicen en los departamentos del GAD Municipal del Cantón Salcedo.

9.1.2. Mecanismos de seguridad asociados a servicios en red.

- El encargado del departamento de sistema tendrá que cumplir la tarea de monitoreo en el rendimiento y capacidad de los servicios que tienen contratados por proveedores, los servicios deberán incluir VPN, firewall, anti intrusos que se desarrollaran dentro del GAD Municipal del Cantón Salcedo o serán adquiridos de manera externa.
- Los servicios de red deben tener controles de autentificación, acceso, cifrado y requerimientos para una conexión segura establecida.

9.1.3. Segregación de redes.

- Los segmentos utilizados en la red dentro del GAD Municipal del Cantón Salcedo serán documentados con un perímetro de seguridad, adicional se deberá configurar redes virtuales, políticas de control de acceso complementadas con puertas de enlace y firewall.
- Al segregar las redes a través de enrutamiento y switching se tendrá como resultado un mejor manejo del tráfico entre los segmentos y sus configuraciones del mismo. Dentro del Municipio se podrá segregar las redes por Vlan para todos los departamentos que la conformen.

9.2. Intercambio de información con partes externas

9.2.1. Políticas y procedimientos de intercambio de información.

- Se tendrá el medio de transmisión de la información al momento de transferirla a organismos externos, si es de manera manual se entregará personalmente al destinatario en un sobre sellado.
- Si el intercambio es vía email se realizará por el correo de la plataforma del GAD Municipal del Cantón Salcedo 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.
- Si el intercambio es por otro medio cumplirá la política de control de acceso y seguridad de red.
- La transmisión de información vía telefónica está prohibida.

- Si el intercambio de información es entre sistemas se debe realizar decretos externos este documento aprueba y define la prestación de servicios mutuos para su cumplimiento de las obligaciones, costos, incumplimientos y responsabilidades, este representada como un documento público que aprueba el convenio de cooperación o de interoperabilidad.

9.2.2. Acuerdos de intercambio.

- La información que se va a transferir pasará por una previa autorización, y esta deberá transmitir solo la información requerida.
- Si la trasmisión es vía email será encriptada establecida con acuerdos de confidencialidad de la información entre departamentos externos y internos.

9.2.3. Mensajería electrónica.

- Se implantará el correo institucional para el GAD Municipal del Cantón Salcedo para poder enviar y recibir información donde el departamento de sistemas mantendrá el monitoreo del servidor de correo, se verán obligados todos los empleados a utilizar este medio de comunicación dentro de su lugar de trabajo.

9.2.4. Acuerdos de confidencialidad y secreto.

- El encargado del departamento de sistemas designará la responsabilidad que permitirá la revisión continua de los acuerdos de confidencialidad a los encargados de cada departamento del GAD Municipal del Cantón Salcedo, el cual podrá revisar, analizar y podrán realizar los cambios en los acuerdos.

10. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.

Objetivo: garantizar que la seguridad de la información sea una parte integral de los sistemas de información en todo el ciclo de vida, incluyendo los requisitos para aquellos que proporcionan servicios en redes públicas, además garantizar que la seguridad de la información se diseñe e implemente dentro del ciclo de vida de desarrollo de los sistemas de información [11].

10.1. Requisitos de seguridad de los sistemas de información.

10.1.1. Análisis y especificación de los requisitos de seguridad.

- El análisis y diseño de los sistemas que funcionan en el GAD Municipal del Cantón Salcedo, deberán contar con mecanismos de seguridad de la información cumpliendo además de los requerimientos del usuario final. Se deberá analizar los riesgos posibles antes de la implementación definiendo así los procedimientos apropiados de seguridad.

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

- Se protegerá la información que pasa a través de las aplicaciones que utilizan redes públicas para transferirla, mediante la encriptación evitando el ingreso no autorizado, el departamento de sistemas analizara los servicios de redes públicas para evaluar los riesgos y vulnerabilidades, dando la mejor solución para proteger la información.

10.1.3. Protección de las transacciones por redes telemáticas.

- Se realizará revisiones continuas de los sistemas verificando su correcto funcionamiento y el almacenamiento de la información, obteniendo los resultados del almacenamiento correcto evitando errores, clonación de la información.

10.2. Seguridad de los procesos de desarrollo y soporte

10.2.1. Política de desarrollo seguro de software.

- Se tendrá un estándar del desarrollo del software a través de ciclos, dependiendo de la metodología, estándares de seguridad y calidad aplicada en el GAD Municipal del Cantón Salcedo donde todas estas políticas estarán documentadas y autorizadas por el departamento de sistemas.

- Los programadores serán responsables de la seguridad del proyecto o del entorno de soporte y deben garantizar que todas las propuestas de cambio en los sistemas serán revisadas para verificar que no comprometan la seguridad del sistema y exista fuga de información.

10.2.2. Procedimientos de control de cambios en los sistemas.

- Los cambios deben ser pasados por escrito al personal del departamento de sistemas en el caso que se necesite modificar datos, se deberá tener en cuenta la autorización e identificación de los elementos que se modificaran como base de datos, hardware o software.
- Se tendrá una auditoria sobre encargados en realizar este tipo de labor dentro del departamento de sistemas ya que solo en este lugar se llevaría a cabo donde serán aprobados y probados.
- En el momento de realizar los cambios se debe garantizar que no sea interrumpida la labor de los servicios que operan en los departamentos, adicional se comunicara con anticipación cobre los cambios a todo el personal del departamento donde se lo realizara.

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

- Se realizará pruebas de funcionamiento a la vez serán monitoreados donde sea necesario de actualizaciones o modificaciones, esto se deberá realizar sin interrupciones en el sistema.

10.2.4. Restricciones a los cambios en los paquetes de software.

- El encargado del departamento de sistemas evaluara las modificaciones de los paquetes que necesiten cambios si son necesario, esto no afectaran la integridad, confidencialidad y disponibilidad de la información, los cambios realizados serán autorizados por el encargado del departamento de sistema.

10.2.5. Uso de principios de ingeniería en protección de sistemas.

- El encargado del departamento de sistema asignará al responsable para la investigación e implementación de los principios de seguridad este deberá analizar previamente los sistemas de información para su implementación.

10.2.6. Seguridad en entornos de desarrollo.

- Se creará un entorno para el desarrollo de software adecuado, según las políticas de control de acceso y seguridades físicas y ambientales para los equipos que se utilizaran para el desarrollo, además el ambiente deberá ser confortable para realizar la labor siendo del agrado de los desarrolladores.

10.2.7. Externalización del desarrollo de software.

- El responsable del monitoreo de las actividades de desarrollo estará al pendiente de las actividades del desarrollo del software externas, es importante que los involucrados en el proyecto tengan en cuenta la creación, innovación, producto u objeto que se desarrolló dentro del GAD Municipal del Cantón Salcedo será propiedad exclusiva del mismo.
- Todo los productos o programas externalizados deberán ser entregados en el tiempo acordado, incluyendo manuales, descripción técnica y documentación respectiva.

10.2.8. Pruebas de funcionalidad durante el desarrollo de los sistemas.

- Se tendrá una lista de planificación de pruebas con usuarios que pertenezca a los departamentos en el caso que sea el sistema para el correspondiente, donde se evaluará los niveles de seguridad en los sistemas y se podrá tomar decisiones a través de los criterios para proteger la información, y se deberá documentar todo lo realizado con sus fechas respectivas y observaciones que hayan manifestado los usuarios.

10.2.9. Pruebas de aceptación.

- Se coordinará un responsable para elaborar un plan de pruebas que deberá ser autorizado y aprobado por el encargado del departamento de sistemas, en el proceso de las pruebas estas deberán dar las incidencias, mejoras, detección de vulnerabilidades y serán registras en un documento o acta.

En el ANEXO 8 se encuentra el formulario de “los sistemas de información”.

10.3. Datos de prueba

10.3.1. Protección de los datos utilizados en pruebas.

- El acceso a la base de datos formal será restringido para hacer pruebas, en el caso de requerir una base de datos generar una con una herramienta que sea prueba o de la misma manera realizar un backup de la misma y notificar que será utilizada para un proyecto en desarrollo.

11. RELACIONES CON SUMINISTRADORES.

Objetivo: garantizar la protección de los activos de la organización que son accesibles a proveedores y mantener el nivel en la prestación de servicios conforme a los acuerdos con el proveedor en materia de seguridad de información [11].

11.1. Seguridad de la información en las relaciones con suministradores

11.1.1. Política de seguridad de la información para suministradores.

- Se analizará los riesgos a la que está expuesta la información de accesos no autorizados por terceros, donde se establecerá los requerimientos de seguridad en aprobación del encargado del departamento de sistemas y deberán ser documentados y actualizadas en el momento que se lo requiera.

11.1.2. Tratamiento del riesgo dentro de acuerdos de suministradores.

- Se establecerá los requerimientos de seguridad de la información para terceras personas que tengan acceso a las TIC´S dentro del GAD Municipal del Cantón Salcedo y que deban dar un tipo de soporte solo con su personal autorizado.
  Los suministros para realizar los mantenimientos serán del GAD Municipal del Cantón Salcedo, para asegurar que la información no sea filtrada por terceros.

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

- El encargado del departamento de sistemas elaborará un manual de procedimientos para proteger la información, la que servirá para la adquisición de suministros informáticos a proveedores en el mercado tecnológico.

11.2. Gestión de la prestación de servicios por suministradores.

11.2.1. Supervisión y revisión de los servicios prestados por terceros.

- Sera obligatorio hacer auditorías a los servicios que este contratados de terceros, para verificar que se trabaje con la información necesaria y que su funcionamiento sea el más óptimo para el GAD Municipal del Cantón Salcedo.
- Adicional se deberá monitorear los servicios y generar registros de la información que se manejen en cambios que se realicen en estos servicios, este plan tendrá como supervisor un encargado del departamento de sistemas.

11.2.2. Gestión de cambios en los servicios prestados por terceros.

- Se registrará los cambios que se realicen para optimizar los servicios del departamento de sistemas, tanto como desarrollar, modificar políticas y procedimientos se puede implementar controles nuevos para el mejoramiento de la seguridad de la información.

12. GESTIÓN DE LOS INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

Objetivo: Garantizar una administración de incidentes de seguridad de la información coherente y eficaz en base a un enfoque de comunicación de los eventos y las debilidades de seguridad [11].

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

12.1.1. Responsabilidades y procedimientos.

- Se capacitará a todos los empleados de los departamentos del GAD Municipal del Cantón Salcedo, sobre la funcionalidad de los sistemas de información para que puedan informar sobre un evento o vulnerabilidad que sea encuentre y que pueda afectar a la seguridad de la información de su área de trabajo o a nivel general.
- El encargado del departamento de sistemas será el responsable de aplicar los procedimientos necesarios para gestionar los incidentes de la información de todo tipo en todo el palacio municipal.

12.1.2. Notificación de los eventos de seguridad de la información.

- El encargado del departamento de sistemas debe notificar a los encargados de los diferentes departamentos acerca de los eventos de seguridad de la información implementados o que serán actualizados para evitar errores al manipular la información.
- Se notificará a través de vía correo electrónico de la institución o grupos creados en las redes sociales en el caso que los empleados no tengan conocimientos sobre cómo utilizar estos medios se debe realizar capacitaciones para la sociabilización.

12.1.3. Notificación de puntos débiles de la seguridad.

- Se implementará una cuenta de correo para soporte, en la que los usuarios podrán reportar vulnerabilidades sospechosas o algún evento fuera de lo común, con toda la información posible para ser analizada.
- La administración de este correo lo deberá realizar los encargados del departamento donde este laborando, en un caso que este fuera de sus manos por una fuerte gravedad, se deberá contactarse con la persona encargada en el departamento de sistemas en un plazo máximo de 48 horas, para recopilar la información necesaria para el análisis del problema.

  En el ANEXO 6 se encuentra el formulario de “Tratamiento y valoración de incidentes”.

- Luego de la recolección de la información del inconveniente el encargado del departamento de sistemas deberá analizar los recopilado.

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

Con la realización de este control es obligatorio aplicar la política de notificación de puntos vulnerables de la seguridad, el siguiente paso será el análisis y podemos clasificarla de la siguiente manera:

- Se trata de una amenaza: se informa y reporta sobre una amenaza y se cierra el registro.
- Se trata de una debilidad: se realiza los 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.
- Se Produjo y debe ser clasificado como un incidente: se activa el proceso de gestión de incidentes.

12.1.5. Respuesta a los incidentes de seguridad.

Con el cumplimiento de este control el encargado de cada departamento deberá notificar sobre los inconvenientes el cual tendrá un periodo de 48 horas para comunicarse con el empleado que lo notifico y seguir con los procedimientos para su análisis y deberá desarrollar acciones inmediatas como:

- Iniciar los procedimientos para evitar que se propaguen los daños o efectos del inconveniente.
- Reclasificar los inconvenientes de acuerdo a la política de valoración de eventos de seguridad de la información.
- Tener el registro recopiladas durante su gestión a través de evidencias.
- Documentar todo sobre el problema ocurrido para tomar decisiones en caso de que vuelva a ocurrir.

12.1.6. Aprendizaje de los incidentes de seguridad de la información.

- El encargado del departamento de sistemas deberá hacer una revisión periódica de los problemas atendidos en un periodo de tiempo, teniendo en cuenta los inconvenientes que han ocurrido con frecuencia en la información, teniendo en cuenta el resultado obtenido, solución y tratamiento dependiendo del tipo, volumen y costo de los incidentes.

12.1.7. Recopilación de evidencias.

- Es obligatorio documentar los incidentes de acuerdo a la plantilla para el tratamiento y valoración del inconveniente, el documento original deberá ser documentado y crear una bitácora digital de los incidentes y su solución para facilitar el acceso a la información y la búsqueda.

13. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.

Objetivo: mantener la seguridad de la información integrada en los sistemas de gestión de continuidad del negocio de la organización y garantizar la disponibilidad de las instalaciones de procesamiento de información [11].

13.1. Continuidad de seguridad de la Información.

13.1.1. Planificación de la continuidad de la seguridad de la información.

- El encargado del departamento de sistemas se compromete a continuar con el plan de seguridad de la información, identificando y comprendiendo las vulnerabilidades que pueda estar expuesto el GAD Municipal del Cantón Salcedo, el mismo tendrá en cuenta las interrupciones en el funcionamiento correcto de los sistemas de información, en tal caso, que un incidente ocurra se tomara en cuenta las precauciones de gestión de riesgos.

13.1.2. Implantación de la continuidad de la seguridad de la información.

- Se identificará los recursos humanos, tecnológicos ambientales y financieros para garantizar los recursos mencionados estos deberán ser archivados para garantizar el nivel de seguridad de la información, este se detallará en responsabilidades, funcionalidades y actividades en caso de situaciones adversas a todos los trabajadores que participe en el sistema de seguridad de la información.

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

- Se verificará los controles cada 6 meses, se debe ejecutar pruebas que involucren a los empleados de todos los departamentos y garantizar que estén capacitados con los conocimientos ante una situación advera.
- Para ponerlo en práctica se podrá realizar un simulacro con las consecuencias reales, para verificar la eficacia y realidad de los controles y se la conclusión de la prueba será registrada para seguir mejorando con nuevas acciones.

13.2. Redundancias.

13.2.1. Disponibilidad de instalaciones para el procesamiento de información.

- Se planificará y se realizará los planos necesarios para la construcción de un área de procesamiento de información donde se verá involucrada nuevas tecnologías y la implementación de nuevos equipos, estas instalaciones de procesamiento de información deben estar aptas para la implementación de controles de seguridad.

14. CUMPLIMIENTO.

Objetivo: garantizar que se implementa y opera la seguridad de la información de acuerdo a las políticas y procedimientos organizacionales Y evitar incumplimientos a requisitos relacionados con la seguridad de la información de cualquier tipo especialmente a las obligaciones legales, estatutarias, normativas o contractuales [11].

14.1. Cumplimiento de los requisitos legales y contractuales.

14.1.1. Identificación de la legislación aplicable.

- Un de los encargados del departamento de sistemas mantendrá actualizada y adaptara las normas y estatutos legales que rigen en el país en especial las que involucran tratamiento de información y/o tengan relación con la tecnología de la información.

14.1.2. Derechos de propiedad intelectual (DPI).

- Una de las personas encargadas del departamento de sistemas y las normas y estatutos también tendrá conocimiento de los requisitos legislativos, normativos

y contractuales de la propiedad intelectual que permitirán el desarrollo y/o creación, implementaciones de software.

14.1.3. Protección de los registros de la organización.

- Los reglamentos, normas y estatutos internos del GAD Municipal del Cantón Salcedo serán actualizados, a través del personal encargada de este ámbito que se encuentre al tanto de esta información, y deberá mantener una capacitación de los reglamentos pertinentes.

14.1.4. Protección de datos y privacidad de la información personal.

- Las bases de datos del GAD Municipal del Cantón Salcedo contará con protección para usuario q permitirán asegurar los datos. Adicional todos los equipos de cómputo pertenecientes a los diferentes departamentos del municipio y que son utilizados por el personal estarán protegidos contra accesos no autorizados.

14.1.5. Regulación de los controles criptográficos.

- Se diseñaran políticas de seguridad que involucren controles criptográficos que permitan salvaguardar la información ante manipulación no autorizada, utilizando un algoritmo de encriptación.

14.2. Revisiones de la seguridad de la información

14.2.1. Revisión independiente de la seguridad de la información.

- Se realizará un análisis de las políticas que dará como resultado preservar los niveles de seguridad de la información. Este análisis debe ser realizado por el departamento de sistemas del GAD Municipal del Cantón Salcedo y que se obtendrá las políticas de seguridad que se deben aplicar dentro del

establecimiento, partiendo de los niveles de criticidad acceso, la ubicación física de las TIC's, y de la información.

14.2.2. Cumplimiento de las políticas y normas de seguridad.

- El encargado del departamento de sistemas y encargados de cada departamento, realizar una auditoría para el cumplimiento de los procedimientos en cuanto a las políticas de seguridad de la información, normas o estatutos que rigen dentro del GAD Municipal del Cantón Salcedo.

14.2.3. Comprobación del cumplimiento.

- Se realizarán simulacros en los sistemas de información para verificar que se cumplan las políticas de seguridad, que se aplican dentro del GAD Municipal del Cantón Salcedo. Donde se tiene que cumplir la confiabilidad, disponibilidad de la información y la integridad de la misma.

Compromiso del GAD Municipal del Cantón Salcedo.

El cumplimento de la norma ISO establecida depende de la partición activa y compromiso que asuma el GAD Municipal del Cantón Salcedo respecto al cumplimiento de continuidad de su ejecución.

Plantilla de Implantación Norma ISO 27002:2013.
Dominio: Numero del Dominio.
Obj. De control: Cantidad y numero del objetivo de control.
Controles: Cantidad y número de controles por cada objetivo.
Orientación: Proporciona información sobre la obligatoriedad de implementar o no el control.
Descripción: Breve descripción de cada objetivo de control agrupándolos por dominio.

PD: Peso del dominio.

NC.D: Nivel de cumplimiento del dominio.

PO: Peso del Objetivo.

NC.O: Nivel del cumplimiento del dominio.

PC: Peso del control.

NC.C: Nivel de cumplimiento del control.

Escala: Escala del cumplimiento

Como utilizar la plantilla de implantación.

Ingrese valores entre 0 y 100 SOLO en los cuadros azules, los cuales corresponderán al valor asignado al nivel de cumplimiento de cada control "NC.C" de la norma; tenga en cuenta que, en esta escala de valoración, el "0" indica que no cumple el control y "100" que lo cumple satisfactoriamente, recuerde que también se puede asignar valores intermedios cuando se cumple parcialmente cualquiera de los controles.

Alto	Más del 70% de cumplimiento
Medio	Entre el 30 y 69 % de cumplimiento
Bajo	Por debajo del 30%

Dominios	Objetivos de Control	Controles	Orientación	Descripción	PD	NC. D	% de cumplimiento de la norma PO	NC. O	PC	NC. C	Escala
	1	2		Políticas de Seguridad	1,75	75	100				
5		2		Política de Seguridad de la Información			100	75			
	1	1	Debe	Documento de la política de seguridad de la información					50	75	
		2	Debe	Revisión de la política de seguridad de la información					50	75	
	2	7		Estructura organizativa para la seguridad	6,14	157,15	100				
		5		Organización interna			71,43	142,86			
		1	Debe	Asignacion de responsabilidades para la seguridad de la informacion					14,2857	100	
		2	Debe	Segregacion de tareas					14,2857	75	
	1	3	Debe	Contacto con las autoridades					14,2857	75	
6		4	Debe	Contacto con grupos de interes especial					14,2857	75	
		5	Debe	Seguridad de la informacion en la gestion de proyectos					14,2857	75	
		2		Dispositivos para movilidad y teletrabajo			28,57	14,29			
	2	1	Debe	Politica de uso de dispositivos para movilidad					14,2857	50	
		2	Debe	Teletrabajo					14,2857	50	
	3	6		Seguridad Recursos Humanos	5,26	81,3	100				
		2		Antes de la contratacion			33,33	16,67			
	1	1	Debe	Investigacion de antecedentes					16,6666	50	
		2	Debe	Terminos y condiciones de contratacion					16,6666	50	
		3		Durante la contratacion			50	56,25			
7	2	1	Debe	Responsabilidad de gestion					16,6666	75	
		2	Debe	Concienciacion, educacion y capacitacion en seguridad de la informacion					16,6666	75	
		3	Debe	Proceso disciplinario					16,6666	75	
	3	1		Cese o cambio de puesto de trabajo			16,67	8,34			
		1	Debe	Cese o cambio de puesto de trabajo					16,6666	100	
	3	10		Gestion de Activos	8,77	115	100				
		4		Responsabilidad sobre los activos			40	70			
		1	Debe	Inventario de activos					10	100	
	1	2	Debe	propiedad de los activos					10	100	
		3	Debe	uso aceptable de los activos					10	100	
		4	Debe	devolucion de activos					10	50	
8		3		Clasificacion de la informacion			30	22,5			
	2	1	Debe	Directrices de clasificacion					10	50	
		2	Debe	Etiquetado y manipulacion de la informacion					10	50	
		3	Debe	Manipulacion de activos					10	50	
		3		Manejo de los soportes de almacenamiento			30	22,5			
	3	1	Debe	Gestion de soportes extraibles					10	50	
		2	Debe	Eliminacion de soportes					10	50	
		3	Debe	Soportes fisicos en transito					10	50	
	4	14		Control de Accesos	12,28	221,4	100				
		2		Requisitos de negocios para el control de accesos			14,29	7,15			
	1	1	Debe	Politica de control de accesos					7,1428	50	
		2	Debe	Control de acceso a las redes y servicios asociados					7,1428	50	
		6		Gestion de acceso de usuario			42,86	123,22			
		1	Debe	Gestion de altas/bajas en el registro de usuarios					7,1428	100	
		2	Debe	gestion de los derechos en acceso asignados a usuarios					7,1428	100	
		3	Debe	gestion de los derechos de acceso con privilegios especiales					7,1428	100	
		4	Debe	gestion de informacion confidencial de autenticacion de usuarios					7,1428	100	
9		5	Debe	revision de los derechos de acceso de los usuarios					7,1428	100	
	2	6	Debe	retirada o adaptacion de los derechos de acceso					7,1428	75	
		1		Responsabilidades del usuario			7,14	1,79			
	3	1	Debe	uso de informacion confidencial para la autenticacion					7,1428	50	
		5		Control de acceso a sistemas y aplicaciones			35,71	89,28			
		1	Debe	restriccion del acceso a la informacion					7,1428	100	
		2	Debe	procedimientos seguros de inicio de sesion					7,1428	100	
		3	Debe	gestion de contraseñas de usuarios					7,1428	100	
		4	Debe	uso de herramientas de administracion de sistemas					7,1428	100	
	4	5	Debe	control de acceso al codigo fuente de los programas.					7,1428	100	
	1	2		Cifrado	1,75	0	100				
10		2		Controles criptograficos			100				
	1	1	Debe	politica de uso de los controles criptograficos					50	50	
		2	Debe	gestion de claves					50	50	
	2	15		Seguridad fisica y ambiental.	13,16	242,5	100				
		6		Area Seguras			40	85			
		1	Debe	perimetro de seguridad fisica					6,6666	50	
		2	Debe	controles fisicos de entrada					6,6666	50	
	1	3	Debe	seguridad de oficinas, despachos y recursos					6,6666	75	
		4	Debe	proteccion contra las amenazas externas y ambientales					6,6666	100	
		5	Debe	el trabajo en areas seguras					6,6666	75	
		6	Debe	areas de acceso publico, carga y descarga					6,6666	75	
		9		Seguridad de los equipos			60	157,5			
11		1	Debe	emplazamiento y proteccion de equipos					6,6666	75	
		2	Debe	instalaciones de suministro					6,6666	100	
		3	Debe	seguridad del cableado					6,6666	50	
		4	Debe	mantenimiento de los equipos					6,6666	50	
	2	5	Debe	salida de activos fuera de las dependencias de la empresa					6,6666	50	
		6	Debe	seguridad de los equipos y activos fuera de las instalaciones					6,6666	50	
		7	Debe	reutilizacion o retirada segura de dispositivos de almacenamiento					6,6666	50	
		8	Debe	equipo informatico de usuario desatendido					6,6666	50	

		9	Debe	politica de puesto de trabajo despejado y bloqueo de pantalla				6,6666	50	
12	7	14		Seguridad en la operativa	12,28	138,4	99,99			
		4		Responsabilidad y pprocedimientos de operación			28,57	57,14		
	1	1	Debe	documentacion de procedimientos de operación				7,1428	100	
		2	Debe	gestion de cambios				7,1428	100	
		3	Debe	gestion de capacidades				7,1428	100	
		4	Debe	separacion de entorno de desarrollo, prueba y produccion				7,1428	100	
	2	1		Proteccion contra codigo malicioso			7,14	3,57		
		1	Debe	controles contra el codigo malicioso				7,1428	100	
	3	1		Copias de Seguridad			7,14	3,57		
		1	Debe	copias de seguridad de la informacion				7,1428	100	
		4		Registro de actividad y supervicion			28,57	57,14		
	4	1	Debe	registro y gestion de eventos de actividad				7,1428	100	
		2	Debe	proteccion de los registros de informacion				7,1428	100	
		3	Debe	registros de actividad de administrador y operador del sistema				7,1428	100	
		4	Debe	sincronizacion de relojes				7,1428	100	
	5	1		Control de software en explotacion			7,14	3,57		
		1	Debe	instalacion del software en sistemas en produccion				7,1428	100	
	6	2		Gestion de la vulnerabilidad tecnica			14,29	10,72		
		1	Debe	gestion de las vulnerabilidades tecnicas				7,1428	75	
		2	Debe	restriccion en la instalacion de software				7,1428	75	
	7	1		Consideraciones de las auditorias de los sistemas de informacion			7,14	2,68		
		1	Debe	controles de auditoria de los sistemas de informacion				7,1428	75	
	2	7		Seguridad en las telecomunicaciones	6,14	167,86	100			
		3		Gestion de la seguridad en las redes			42,86	53,58		
	1	1	Debe	controles de red				14,2857	100	
		2	Debe	mecanismos de seguridad asociados a servicios en red				14,2857	75	
13		3	Debe	segregacion de redes				14,2857	75	
		4		Intercambio de informacion con partes externas			57,14	114,28		
	2	1	Debe	politicas y procedimientos de intercambio de informacion				14,2857	100	
		2	Debe	acuerdos de intercambio				14,2857	100	
		3	Debe	mensajeria electronica				14,2857	100	
		4	Debe	acuerdos de confidencialidad y secreto				14,2857	100	
	3	13		Adquisicion, desarrollo y mantenimiento de los sistemas de informacion	11,4	379,7	100			
		3		Requisitos de seguridad de los sistemas de informacion			23,08	64,28		
	1	1	Debe	analisis y especificacion de los requisitos de seguridad				7,6923	100	
		2	Debe	seguridad de las comunicaciones en servicios accesibles por redes publicas				7,6923	75	
		3	Debe	proteccion de las trasacciones por redes telematicas				7,6923	50	
		9		Seguridad en los procesos de desarrollo y soporte			69,23	311,54		
		1	Debe	politica de desarrollo seguro de software				7,6923	100	
		2	Debe	procedimientos de control de cambios en los sistemas				7,6923	100	
14		3	Debe	revision tecnica de las aplicaciones tras cambios en el SO				7,6923	100	
	2	4	Debe	restricciones a los cambios en los paquetes de software				7,6923	100	
		5	Debe	uso de principios de ingenieria en proteccion de sistemas				7,6923	100	
		6	Debe	seguridad en entornos de desarrollo				7,6923	100	
		7	Debe	externalizacion del desarrollo de software				7,6923	100	
		8	Debe	pruebas de funcionalidad durante el desarrollo de los sistemas				7,6923	100	
		9	Debe	pruebas de aceptacion				7,6923	100	
	3	1		Datos de Prueba			7,69	3,85		
		1	Debe	proteccion de los datos utilizados en pruebas				7,6923	100	
	2	5		Relaciones con suministradores	4,39	85	100			
		3		Seguridad de la informacion en las relaciones con suministradores			60	45		
	1	1	Debe	politica de seguridad de la informacion para suministradores				20	50	
15		2	Debe	tratamiento del riesgo dentro de acuerdos de suministradores				20	50	

		3	Debe	cadena de suministro en tecnologias de la informacion y comunicación					20	50	
	2	2		Gestion de la prestacion del servicio por suministradores			40	40			
		1	Debe	supervision y revision de los servicios prestados por terceros					20	100	
		2	Debe	gestion de cambios en los servicios prestador por terceros					20	100	
16	1	7		Gestion de incidentes en la seguridad de la informacion	6,14	350	100				
		7		Gestion de incidentes en la seguridad de la informacion			100	350			
		1	Debe	responsabilidad y procedimientos					14,2857	100	
		2	Debe	notificacion de los eventos de seguridad de la informacion					14,2857	100	
	1	3	Debe	notificacion de puntos debiles de la seguridad					14,2857	100	
		4	Debe	valoracion de eventos de seguridad de la informacion y toma de decisiones					14,2857	100	
		5	Debe	repuesta a los incidentes de seguridad					14,2857	100	
		6	Debe	aprendizaje de los incidentes de seguridad de la informacion					14,2857	100	
		7	Debe	recopilacion de evidencias					14,2857	100	
17	2	4		informacion en la gestion de continuidad	3,51	125	100				
	1	3		Continundad de la seguridad de la informacion			75	112,5			
		1	Debe	planificacion de la continuidad de la seguridad de la informacion					25	100	
		2	Debe	implantacion de la continuidad de la seguridad de la informacion					25	100	
		3	Debe	verificacion, revision y evaluacion de la continuidad de la seguridad de la informacion					25	100	
	2	1		Redundancias			25	12,5			
		1	Debe	disponibilidad de instalaciones para el procesamiento de la informacion					25	100	
18	2	8		Cumplimiento	7,02	189,06	100				
	1	5		Cumplimiento de los requisitos legales y contractuales			62,5	132,81			
		1	Debe	identificacion de la legislacion aplicable					12,5	75	
		2	Debe	derechos de propiedad intelectual					12,5	75	
		3	Debe	proteccion de los registros de la organización					12,5	100	
		4	Debe	proteccion de datos y privacidad de la informacion personal					12,5	100	
		5	Debe	regulacion de los controles criptograficos					12,5	75	
	2	3		Revisiones de la seguridad de la informacion			37,5	56,25			
		1	Debe	revision independiente de la seguridad de la informacion					12,5	100	
		2	Debe	cumplimiento de las politicas y normas de seguridad					12,5	100	
		3	Debe	comprobacion del cumplimiento					12,5	100	
Dominios		14									
Objetivos de control		35									
Controles		114									

Gráfico Nº 6: Plantilla de implantación Norma ISO en el GAD Municipal del Cantón Salcedo.

Elaborado por: Sandra Criollo.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- El personal administrativo de cada departamento realizara sus funciones acordes a los servicios del GAD Municipal del Cantón Salcedo, por lo que, es importante que la información y centros de procesamiento tengan restringido el acceso a personas ajenas, estableciendo lineamientos de seguridad para la información en base a la norma ISO 27002:2013, ya que las políticas de seguridad minimizan la pérdida de información y garantizando el funcionamiento de los procesos.

- Debido a que la tecnología evolucionada a diario, el departamento de sistemas del GAD Municipal del Cantón Salcedo deberá estar constantemente actualizada en los ámbitos de tecnología, telecomunicaciones y políticas de seguridad, aplicando procedimientos, documentación y manuales para la estandarización de los procesos.

- El análisis de la situación actual se realizó en base a encuestas por lo que fue necesaria la colaboración del personal de cada departamento, ya que son ellos quienes trabajan día a día en su labor dentro del GAD Municipal del Cantón Salcedo y conocen a detalle sus recursos, fortalezas y debilidades.

- La implantación de la norma ISO que se propuso en este plan se elaboró en base de las necesidades del GAD Municipal del Cantón Salcedo y detalla los recursos reales necesarios y que buscan mejorar los servicios que ofrece el mismo y por ende contribuir con el crecimiento y excelencia.

- El presente proyecto es el primero de este tipo que se elabora del GAD Municipal del Cantón Salcedo, es por ello que la implantación basada en el plan desarrollado dejará un precedente sobre la administración de la información y que podrá ir mejorando con el tiempo

- El departamento de sistemas del GAD Municipal del Cantón Salcedo, afrontara con las deficiencias de seguridad de la información, basadas en el documento y realizar enmendaduras a través de las políticas de seguridad.

5.2 RECOMENDACIONES

- Se recomienda continuar con campañas de capacitación a los empleados de cada departamento que se verán involucrados en los procesos dentro del GAD Municipal del Cantón Salcedo, para crear una cultura de colaboración y asistencia en la seguridad, así como para la implantación de futuras mejoras en cada departamento.

- El Departamento de sistemas debe profundizar el conocimiento de la Norma ISO 27002:2013, para contar con la asistencia de personal capacitado; 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 y la difusión de las mismas a todos los funcionarios y empleados del GAD Municipal del Cantón Salcedo, 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.

- El recurso humano es muy importante dentro del GAD Municipal del Cantón Salcedo, es por ello que los proyectos propuestos buscan la mejora de la calidad

de su trabajo por eso recomienda la activa colaboración en todos ellos ya que serán para su beneficio.

- Aprobar y poner en marcha manuales de políticas y normas de seguridad informática.

- El departamento de recursos humanos, deberá constatar una clara y eficiente información sobre el individuo en proceso de reclutamiento, debiendo poner mucha más atención en que cada uno de los miembros del personal tengan los conocimientos necesarios para el cargo que desempeñara.

- Es recomendable que dentro del GAD Municipal del Cantón Salcedo se elabore planes de contingencia el mismo que le permitirá reaccionar de manera adecuada ante una crisis de seguridad.

- Realizar grandes cambios en el sistema de backups puede ser complejo, por lo que es importante realizar un buen estudio para escoger la mejor opción. La clave se encuentra en definir y cubrir las necesidades de cada plataforma ajustando el sistema a los recursos disponibles.

BIBLIOGRAFÌA

[1] Guía Comercial de Quito, “Seguridad Informática.” 2015. [en línea]. Disponible en: www.guiaccq.com/product/index/403/.

[2] Ernst & Young, “Seguridad de la información en un mundo sin fronteras.” 2011. [en línea]. Disponible en: www.ey.com/Publication/vwLUAssets/Seguridad_de_la_informacion_en_un_mundo_sin_fronteras/$FILE/Seguridad_de_la_informacion_en_un_mundo_sin_fronteras.pdf/.

[3] E.Torres, “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.” 2015. [en línea]. Disponible en: www.repo.uta.edu.ec/bitstream/123456789/13057/1/Tesis_t1030si.pdf/.

[4] W. Fuertes, “Evaluación técnicas de la seguridad informática del Data Center de la Escuela Politécnica del Ejercito.” 2011. [en línea]. Disponible en: www.repositorio.espe.edu.ec/handle/21000/4279/.

[5] S. Paillacho, “Modelo de un proceso de la gestión del riesgo de la seguridad de la información en entidades gubernamentales.” 2015. [en línea]. Disponible en: www.bibdigital.epn.edu.ec/bitstream/15000/10653/1/CD-6286.pdf/.

[6] Y. Garcia, “Modelo de gestión de la seguridad de la información en los procesos críticos de las áreas financieras universitaria. Caso Puce.” 2015. [en línea]. Disponible en: www.bibdigital.epn.edu.ec/handle/15000/10537?mode=full/.

[7] J. Jarauta, J.Sierra, R.Palacios “Seguridad Informática” 2006. [en línea]. Disponible en: www.iit.upcomillas.es/palacios/seguridad/cap01.pdf/.

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

[9] ISOTools Excellence, “Blog especializado en sistemas de gestión de seguridad de la información.” 2015. [en línea]. Disponible en: www.pmg-ssi.com/2015/07/que-es-sgsi/

[10] R. Echeverria, “Evaluación del sistema de gestión de la seguridad de la informacion de la empresa eléctrica quito utilizando la norma ISO 27001.” 2015. [en línea]. Disponible en: www.bibdigital.epn.edu.ec/bitstream/15000/12000/1/CD-6610.pdf/.

[11] El portal de ISO 27001. [Online]. Disponible en: www.iso27000.es/iso27000.html/.

[12] G. Pallas, M. Corti “Metodología de implantación de un SGSI en grupos empresariales de relación jerárquica” 2014. [en línea]. Disponible en: www.fing.edu.uy/inco/eventos/cibsi09/docs/Papers/CIBSI-Dia2-Sesion3(4).pdf/.

ANEXOS

Anexo 1: ACUERDO DE CONFIDENCIALIDAD

Al objeto de garantizar la confidencialidad la información manejada dentro del GAD Municipal del Cantón Salcedo, se hace necesario la firma de un acuerdo que garantice unos niveles de confianza entre las partes. El documento se firmará una vez aceptado y firmado el acuerdo por ambas partes.

Por lo tanto, ambas partes han resuelto suscribir el presente acuerdo, sujeto a las siguientes cláusulas y condiciones:

1) A partir de la celebración del presente Convenio de Confidencialidad entre las partes, **EL EMPLEADO** trabajará con **LA INFORMACIÓN DEL GAD MUNICIPAL DEL CANTON SALCEDO** sobre la base de un entendimiento expreso fundamental de acuerdo al cual ninguna de las partes se encontrará obligados a celebrar ningún otro contrato con respecto a tal **INFORMACIÓN**.

2) **LA INFORMACIÓN** es de propiedad de **GAD MUNICIPAL DEL CANTON SALCEDO** y el presente Convenio no será interpretado como un otorgamiento a favor del **EMPLEADO** o cualquier otra clase de derechos sobre tal **INFORMACIÓN**.

3) **LA INFORMACION** suministrada, objeto de este convenio no podrá ser difundida, divulgada ni aprovechada por **EL EMPLEADO** fuera del **GAD MUNICIPAL DEL CANTON SALCEDO.**

4) **EL GAD MUNICIPAL DEL CANTON SALCEDO** garantiza que su personal estará sujetas al cumplimiento de todas las cláusulas del presente convenio a toda persona que tenga acceso a la información suministrada, haciéndose este último responsable de todo incumplimiento efectuado por cualquiera de los sujetos referidos en esta cláusula.

5) No podrá ser considerada como confidencial la información que sea susceptible de ser conocida mediante la utilización de canales regulares y legales de información, ni la información que sea de público conocimiento.
De no ser así, se presume que toda información entregada es confidencial, y debe adecuarse a lo establecido en la presente declaración.
11) Para el supuesto de incumplimiento de alguna de las cláusulas que anteceden, la parte cumplidora podrá rescindir el presente acuerdo y/o reclamar los daños y perjuicios sufridos hasta la suspensión laboral del empleado.

12) Para el supuesto caso de controversia en cuanto a los alcances del presente, las partes se someten a la jurisdicción de los tribunales.

13) A todos los efectos legales las partes fijan sus domicilios en los denunciados *ut supra* donde serán válidas todas las notificaciones judiciales y extrajudiciales.

En prueba de conformidad se firman, a los ___ días del mes de _____ de 201_.

_____ _____

EMPLEADO

GAD MUNICIPAL DEL

CANTON SALCEDO

Anexo 2: Formulario de Inventario de Hardware y Software de los computadores

Nombre del equipo	
Dirección IP	
Mascara de Subred	
Nombre de Dominio	
Ubicación física del equipo	
Modelo del Procesador	
Marca	
Modelo	
Número de procesadores	
Velocidad Procesador	
Sistema Operativo	
Versión de Sistema Operativo	
Memoria RAM	
Capacidad de Almacenamiento	
Seriales de los componentes	

Lineamientos de uso de los equipos:

- Cerca de los equipos, no consumir alimentos ni 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 mantenimiento sobre el hardware.
- Conservar los equipos en adecuadas condiciones ambientales.

Anexo 3: Formulario de Solicitud de Acceso a Sistemas de Información

<table>
<tr><td colspan="2">Solitud de acceso a Sistemas de Información</td></tr>
<tr><td colspan="2">Datos Generales</td></tr>
<tr><td>Departamento:</td><td></td></tr>
<tr><td colspan="2">Datos del Usuario</td></tr>
<tr><td colspan="2">Apellido y Nombre del Solicitante:</td></tr>
<tr><td colspan="2">Cargo: Telf.:</td></tr>
<tr><td colspan="2">Correo Electrónico:</td></tr>
<tr><td colspan="2">Perfil de usuario a crear o modificar</td></tr>
<tr><td>Creación</td><td>Modificación</td></tr>
<tr><td>Perfil Nº: ☐</td><td>Eliminación: ☐

Cambio de perfil: ☐</td></tr>
<tr><td colspan="2">Firmantes</td></tr>
<tr><td colspan="2">_____ _____
Cargo: Cargo:
Fecha: Fecha:
Solicitante: Autoriza:</td></tr>
<tr><td colspan="2">Aprobación (Uso Interno del Departamento)</td></tr>
<tr><td colspan="2">_____
Jefe Departamento
Fecha:</td></tr>
<tr><td colspan="2">OBSERVACIÓN:</td></tr>
</table>

Lineamientos:

- El usuario y la contraseña son de uso personal.
- En caso de que el funcionario sea suspendido temporal o definitivamente, se deberá informar de manera inmediata al administrador de usuarios.
- En caso de realizar cambios en el perfil de usuario, se debe informar al Administrador de usuarios.

Anexo 4: Formulario de Creación de usuario y responsabilidad de contraseñas

Solitud de acceso a Sistemas de Información	
Datos Generales	
Departamento**:**	
Datos del Usuario	
Apellido y Nombre del Solicitante:	
Cargo:	Telf.:
Correo Electrónico:	
Perfil de usuario a crear	
Sistema de Información:	
Usuario:	
Contraseña:	
Obligaciones del Usuario	
La clave o contraseña es de uso personal y no puede ser otorgada a otro funcionario por ningún motivo. Para realizar cambios de perfiles de usuario se debe comunicar con el departamento de Sistemas del GAD Municipal del Cantón Salcedo. En caso de que el funcionario sea suspendido temporal o definitivamente de su cargo, se deberá informar de manera inmediata al administrador de usuarios. El funcionario debe cerrar su sesión de usuario cuando no esta no este en uso.	
Firmantes	
_____ **Cargo:** **Fecha:** **Solicitante:**	_____ **Cargo:** **Fecha:** **Autoriza:**
OBSERVACIÓNES:	

Anexo 5: Formulario de Listado de servidores y contraseñas

Listado de Servidores y Contraseñas			
Datos Generales			
Departamento**:**			
Datos del Usuario			
Apellido y Nombre del Solicitante:			
Cargo:		Telf.:	
Correo Electrónico:			
Listado de servidores			
HOSTNAME	**DIRECCION IP**	**USUARIO**	**CONTRASEÑA**
Firmantes			
_____		_____	
Cargo:		**Cargo:**	
Fecha:		**Fecha:**	
Solicitante:		**Autoriza:**	
OBSERVACIÓNES:			

Anexo 6: Formulario para el Tratamiento y Valoración de incidentes

Tratamiento y Valoración de incidentes	
Datos Generales	
Departamento**:**	
Quien lo reporta:	
Nª de incidente:	
Prioridad:	
Usuarios Afectados:	
Datos del Incidente	
Descripción**:**	
Posible Causa:	
Fecha y Hora Aproximada iniciado el incidente:	
Fecha y hora de detección:	
Fecha y hora de restauración:	
Sistemas Afectados:	
Registros/Datos Afectados:	
Protocolos Atacados (HTTP, POP, etc.):	
Objetivo del Sistema Afectado:	
Costos asociados:	
Actividades de Restauración:	
Resolución:	
Firmantes	
_____ **Cargo:** **Fecha:** **Solicitante:**	_____ **Cargo:** **Fecha:** **Autoriza:**
OBSERVACIÓNES:	

Anexo 7: Formato para el registro de Backups.

Código:
Versión:
Fecha de actualización:
Elaborado por:

Sistema de información	Tipo de Backups	Tiempo del Backups	Medio de Almacenamiento	Lugar de Almacenamiento	Persona que lo genera

Anexo 8: Reporte de emergencias

Evento	**Descripción**	**Proceso alterno que debe realizar el usuario del sistema**	**Proceso alterno que debe realizar el personal de sistemas**
Caída del sistema	No hay comunicación en la red local	Realizar las operaciones manualmente	Asignar al personal de sistemas para identificar el problema.
Estación de trabajo no funciona	Posible falla eléctrica en el equipo	Verificar que todo esté bien conectado.	Pedir ayuda al departamento de sistemas