Universidad Nacional Autónoma de México

Facultad de Estudios Superiores Cuautitlán

Gestión de Seguridad Informática en una dependencia gubernamental

T e s i s

Para obtener el título de:

Licenciado en informática

Presenta:
Elvia Lorena Gomez Bravo
Gustavo Duran Cruz

L.I. Lara Martínez Maricela

Cuautitlán Izcalli, Estado de México 2022

Universidad Nacional Autónoma de México
UNAM
Biblioteca Central
Dirección General de Bibliotecas de la UNAM

UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

VNIVERSIDAD NACIONAL AVTÓNOMA DE MEXICO

FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLÁN
SECRETARÍA GENERAL
DEPARTAMENTO DE TITULACIÓN

U.N.A.M.
FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLÁN

ASUNTO: VOTO APROBATORIO

DR. DAVID QUINTANAR GUERRERO
DIRECTOR DE LA FES CUAUTITLAN
PRESENTE

ATN: DRA. MARÍA DEL CARMEN VALDERRAMA BRAVO
Jefa del Departamento de Titulación
de la FES Cuautitlán.

Con base en el Reglamento General de Exámenes, y la Dirección de la Facultad, nos permitimos comunicar a usted que revisamos el trabajo de: **Tesis**

Gestión de Seguridad Informática en una Dependencia Gubernamental

Que presenta la pasante: **Elvia Lorena Gómez Bravo**
Con número de cuenta: **415003043** para obtener el Título de: **Licenciada en Informática**

Considerando que dicho trabajo reúne los requisitos necesarios para ser discutido en el **EXAMEN PROFESIONAL** correspondiente, otorgamos nuestro **VOTO APROBATORIO**.

ATENTAMENTE
"POR MI RAZA HABLARÁ EL ESPÍRITU"
Cuautitlán Izcalli, Méx. a 15 de marzo de 2022.

PROFESORES QUE INTEGRAN EL JURADO

	NOMBRE	FIRMA
PRESIDENTE	Dr. Valentín Roldan Vázquez	
VOCAL	L.I. Maricela Lara Martínez	Maricela Lara
SECRETARIO	M. en C. Antonio Gama Campillo	
1er. SUPLENTE	L.S.C. Liana López Pacheco	
2do. SUPLENTE	M.D.A. Clarisa Clemente Rodríguez	

NOTA: los sinodales suplentes están obligados a presentarse el día y hora del Examen Profesional.

MCVB/javg

VNIVERSIDAD NACIONAL AVTÓNOMA DE MEXICO

FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLÁN
SECRETARÍA GENERAL
DEPARTAMENTO DE TITULACIÓN

U.N.A.M.
FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLÁN

ASUNTO: VOTO APROBATORIO

DR. DAVID QUINTANAR GUERRERO
DIRECTOR DE LA FES CUAUTITLAN
PRESENTE

ATN: DRA. MARÍA DEL CARMEN VALDERRAMA BRAVO
Jefa del Departamento de Titulación
de la FES Cuautitlán.

Con base en el Reglamento General de Exámenes, y la Dirección de la Facultad, nos permitimos comunicar a usted que revisamos el trabajo de: **Tesis**

Gestión de Seguridad Informática en una Dependencia Gubernamental

Que presenta la pasante: **Elvia Lorena Gómez Bravo**
Con número de cuenta: **415003043** para obtener el Título de: **Licenciada en Informática**

Considerando que dicho trabajo reúne los requisitos necesarios para ser discutido en el **EXAMEN PROFESIONAL** correspondiente, otorgamos nuestro **VOTO APROBATORIO**.

ATENTAMENTE
"POR MI RAZA HABLARÁ EL ESPÍRITU"
Cuautitlán Izcalli, Méx. a 15 de marzo de 2022.

PROFESORES QUE INTEGRAN EL JURADO

	NOMBRE	FIRMA
PRESIDENTE	Dr. Valentín Roldan Vázquez	
VOCAL	L.I. Maricela Lara Martínez	Maricela Lara
SECRETARIO	M. en C. Antonio Gama Campillo	
1er. SUPLENTE	L.S.C. Liana López Pacheco	
2do. SUPLENTE	M.D.A. Clarisa Clemente Rodríguez	

NOTA: los sinodales suplentes están obligados a presentarse el día y hora del Examen Profesional.

MCVB/javg

VNIVERSIDAD NACIONAL
AVTÓNOMA DE
MEXICO

FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLÁN
SECRETARÍA GENERAL
DEPARTAMENTO DE TITULACIÓN

U.N.A.M.
FACULTAD DE ESTUDIOS
SUPERIORES CUAUTITLÁN

ASUNTO: VOTO APROBATORIO

DR. DAVID QUINTANAR GUERRERO
DIRECTOR DE LA FES CUAUTITLAN
PRESENTE

ATN: DRA. MARÍA DEL CARMEN VALDERRAMA BRAVO
Jefa del Departamento de Titulación
de la FES Cuautitlán.

Con base en el Reglamento General de Exámenes, y la Dirección de la Facultad, nos permitimos comunicar a usted que revisamos el trabajo de: **Tesis**

Gestión de Seguridad Informática en una Dependencia Gubernamental

Que presenta la pasante: **Elvia Lorena Gómez Bravo**
Con número de cuenta: **415003043** para obtener el Título de: **Licenciada en Informática**

Considerando que dicho trabajo reúne los requisitos necesarios para ser discutido en el **EXAMEN PROFESIONAL** correspondiente, otorgamos nuestro **VOTO APROBATORIO**.

ATENTAMENTE
"POR MI RAZA HABLARÁ EL ESPÍRITU"
Cuautitlán Izcalli, Méx. a 15 de marzo de 2022.

PROFESORES QUE INTEGRAN EL JURADO

	NOMBRE	FIRMA
PRESIDENTE	Dr. Valentín Roldan Vázquez	
VOCAL	L.I. Maricela Lara Martínez	Maricela Lara
SECRETARIO	M. en C. Antonio Gama Campillo	
1er. SUPLENTE	L.S.C. Liana López Pacheco	
2do. SUPLENTE	M.D.A. Clarisa Clemente Rodríguez	

NOTA: los sinodales suplentes están obligados a presentarse el día y hora del Examen Profesional.

MCVB/javg

VNIVERSIDAD NACIONAL AVTÓNOMA DE MEXICO

FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLÁN
SECRETARÍA GENERAL
DEPARTAMENTO DE TITULACIÓN

U.N.A.M.
FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLÁN

ASUNTO: VOTO APROBATORIO

DR. DAVID QUINTANAR GUERRERO
DIRECTOR DE LA FES CUAUTITLAN
PRESENTE

ATN: DRA. MARÍA DEL CARMEN VALDERRAMA BRAVO
Jefa del Departamento de Titulación
de la FES Cuautitlán.

Con base en el Reglamento General de Exámenes, y la Dirección de la Facultad, nos permitimos comunicar a usted que revisamos el trabajo de: **Tesis**

Gestión de Seguridad Informática en una Dependencia Gubernamental

Que presenta la pasante: **Elvia Lorena Gómez Bravo**
Con número de cuenta: **415003043** para obtener el Título de: **Licenciada en Informática**

Considerando que dicho trabajo reúne los requisitos necesarios para ser discutido en el **EXAMEN PROFESIONAL** correspondiente, otorgamos nuestro **VOTO APROBATORIO**.

ATENTAMENTE
"POR MI RAZA HABLARÁ EL ESPÍRITU"
Cuautitlán Izcalli, Méx. a 15 de marzo de 2022.

PROFESORES QUE INTEGRAN EL JURADO

	NOMBRE	FIRMA
PRESIDENTE	Dr. Valentín Roldan Vázquez	
VOCAL	L.I. Maricela Lara Martínez	Maricela Lara
SECRETARIO	M. en C. Antonio Gama Campillo	
1er. SUPLENTE	L.S.C. Liana López Pacheco	
2do. SUPLENTE	M.D.A. Clarisa Clemente Rodríguez	

NOTA: los sinodales suplentes están obligados a presentarse el día y hora del Examen Profesional.

MCVB/javg

VNIVERSIDAD NACIONAL AVPNOMA DE MEXICO

FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLÁN
SECRETARÍA GENERAL
DEPARTAMENTO DE TITULACIÓN

U.N.A.M.
FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLÁN

ASUNTO: VOTO APROBATORIO

DR. DAVID QUINTANAR GUERRERO
DIRECTOR DE LA FES CUAUTITLAN
PRESENTE

ATN: DRA. MARÍA DEL CARMEN VALDERRAMA BRAVO
Jefa del Departamento de Titulación
de la FES Cuautitlán.

Con base en el Reglamento General de Exámenes, y la Dirección de la Facultad, nos permitimos comunicar a usted que revisamos el trabajo de: **Tesis**

Gestión de Seguridad Informática en una Dependencia Gubernamental

Que presenta el pasante: **Gustavo Duran Cruz**
Con número de cuenta: **414089338** para obtener el Título de: **Licenciado en Informática.**

Considerando que dicho trabajo reúne los requisitos necesarios para ser discutido en el **EXAMEN PROFESIONAL** correspondiente, otorgamos nuestro **VOTO APROBATORIO**.

ATENTAMENTE
"POR MI RAZA HABLARÁ EL ESPÍRITU"
Cuautitlán Izcalli, Méx. a 15 de marzo de 2022.

PROFESORES QUE INTEGRAN EL JURADO

	NOMBRE	FIRMA
PRESIDENTE	Dr. Valentín Roldan Vázquez	
VOCAL	L.I. Maricela Lara Martínez	Maricela Lara
SECRETARIO	M. en C. Antonio Gama Campillo	
1er. SUPLENTE	L.S.C. Liana López Pacheco	
2do. SUPLENTE	M.D.A. Clarisa Clemente Rodríguez	

NOTA: los sinodales suplentes están obligados a presentarse el día y hora del Examen Profesional.

MCVB/javg

VNIVERSIDAD NACIONAL AVPNOMA DE MEXICO

FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLÁN
SECRETARÍA GENERAL
DEPARTAMENTO DE TITULACIÓN

U.N.A.M.
FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLÁN

ASUNTO: VOTO APROBATORIO

DR. DAVID QUINTANAR GUERRERO
DIRECTOR DE LA FES CUAUTITLAN
PRESENTE

ATN: DRA. MARÍA DEL CARMEN VALDERRAMA BRAVO
Jefa del Departamento de Titulación
de la FES Cuautitlán.

DEPARTAMENTO DE TITULACIÓN

Con base en el Reglamento General de Exámenes, y la Dirección de la Facultad, nos permitimos comunicar a usted que revisamos el trabajo de: **Tesis**

Gestión de Seguridad Informática en una Dependencia Gubernamental

Que presenta el pasante: **Gustavo Duran Cruz**
Con número de cuenta: **414089338** para obtener el Título de: **Licenciado en Informática.**

Considerando que dicho trabajo reúne los requisitos necesarios para ser discutido en el **EXAMEN PROFESIONAL** correspondiente, otorgamos nuestro **VOTO APROBATORIO**.

ATENTAMENTE
"POR MI RAZA HABLARÁ EL ESPÍRITU"
Cuautitlán Izcalli, Méx. a 15 de marzo de 2022.

PROFESORES QUE INTEGRAN EL JURADO

	NOMBRE	FIRMA
PRESIDENTE	Dr. Valentín Roldan Vázquez	
VOCAL	L.I. Maricela Lara Martínez	Maricela Lara
SECRETARIO	M. en C. Antonio Gama Campillo	
1er. SUPLENTE	L.S.C. Liana López Pacheco	
2do. SUPLENTE	M.D.A. Clarisa Clemente Rodríguez	

NOTA: los sinodales suplentes están obligados a presentarse el día y hora del Examen Profesional.

MCVB/javg

VNIVERSIDAD NACIONAL AVTÓNOMA DE MEXICO

FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLÁN
SECRETARÍA GENERAL
DEPARTAMENTO DE TITULACIÓN

ASUNTO: VOTO APROBATORIO

DR. DAVID QUINTANAR GUERRERO
DIRECTOR DE LA FES CUAUTITLAN
PRESENTE

ATN: DRA. MARÍA DEL CARMEN VALDERRAMA BRAVO
Jefa del Departamento de Titulación
de la FES Cuautitlán.

Con base en el Reglamento General de Exámenes, y la Dirección de la Facultad, nos permitimos comunicar a usted que revisamos el trabajo de: **Tesis**

Gestión de Seguridad Informática en una Dependencia Gubernamental

Que presenta el pasante: **Gustavo Duran Cruz**
Con número de cuenta: **414089338** para obtener el Título de: **Licenciado en Informática.**

Considerando que dicho trabajo reúne los requisitos necesarios para ser discutido en el **EXAMEN PROFESIONAL** correspondiente, otorgamos nuestro **VOTO APROBATORIO.**

ATENTAMENTE
"POR MI RAZA HABLARÁ EL ESPÍRITU"
Cuautitlán Izcalli, Méx. a 15 de marzo de 2022.

PROFESORES QUE INTEGRAN EL JURADO

	NOMBRE	FIRMA
PRESIDENTE	Dr. Valentín Roldan Vázquez	
VOCAL	L.I. Maricela Lara Martínez	Maricela Lara
SECRETARIO	M. en C. Antonio Gama Campillo	
1er. SUPLENTE	L.S.C. Liana López Pacheco	
2do. SUPLENTE	M.D.A. Clarisa Clemente Rodríguez	

NOTA: los sinodales suplentes están obligados a presentarse el día y hora del Examen Profesional.

MCVB/javg

VNIVERSIDAD NACIONAL AVPNOMA DE MEXICO

FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLÁN
SECRETARÍA GENERAL
DEPARTAMENTO DE TITULACIÓN

U.N.A.M.
FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLÁN

ASUNTO: VOTO APROBATORIO

DR. DAVID QUINTANAR GUERRERO
DIRECTOR DE LA FES CUAUTITLAN
PRESENTE

ATN: DRA. MARÍA DEL CARMEN VALDERRAMA BRAVO
Jefa del Departamento de Titulación
de la FES Cuautitlán.

DEPARTAMENTO DE TITULACIÓN

Con base en el Reglamento General de Exámenes, y la Dirección de la Facultad, nos permitimos comunicar a usted que revisamos el trabajo de: **Tesis**

Gestión de Seguridad Informática en una Dependencia Gubernamental

Que presenta el pasante: **Gustavo Duran Cruz**
Con número de cuenta: **414089338** para obtener el Título de: **Licenciado en Informática.**

Considerando que dicho trabajo reúne los requisitos necesarios para ser discutido en el **EXAMEN PROFESIONAL** correspondiente, otorgamos nuestro **VOTO APROBATORIO**.

ATENTAMENTE
"POR MI RAZA HABLARÁ EL ESPÍRITU"
Cuautitlán Izcalli, Méx. a 15 de marzo de 2022.

PROFESORES QUE INTEGRAN EL JURADO

	NOMBRE	FIRMA
PRESIDENTE	Dr. Valentín Roldan Vázquez	
VOCAL	L.I. Maricela Lara Martínez	Maricela Lara
SECRETARIO	M. en C. Antonio Gama Campillo	
1er. SUPLENTE	L.S.C. Liana López Pacheco	
2do. SUPLENTE	M.D.A. Clarisa Clemente Rodríguez	

NOTA: los sinodales suplentes están obligados a presentarse el día y hora del Examen Profesional.

MCVB/javg

Agradecimientos

Mela, sin ti no sería la mujer y profesionista en la que me he convertido, tú me cuidaste y me guiaste hasta aquí. Te gradezco todo lo que hiciste por mí desde niña, cuidados, amor y educación. Daria todo por volvernos a encontrar y mirarte a los ojos y enseñarte todo lo que he logrado, te prometí que un día llegaría a tu lado a decirte “lo logramos” y llego el momento de hacerlo.

Gracias por estar ahí cada que llegaba de la escuela y preocuparte porque llegaba a dormir en vez de comer, por los abrazos, las risas, las bromas y por creer en mí en todos mis sueños por más locos que sonaran, tú siempre confiaste en todo lo que soñé.

Fuiste y siempre serás mi segunda mamá estes en donde estes, eres y siempre serás mi amor eterno gracias por estar siempre estar a mi lado.

Lirona, te agradezco por todos los años de sacrificio que hiciste para brindarme una educación y un techo para vivir. Se que no fue nada fácil hacerlo, pero gracias a eso hoy tengo las armas para seguir adelante y valerme por mi misma, como lo hemos dicho tantas veces, valió la pena cada desmañanada, cada examen de admisión al que me llevaste así fuera del otro lado de la ciudad. Gracias por hacer hasta lo imposible para cubrir los gastos que conlleva estudiar una carrera universitaria, pasajes, materiales y hasta chicarrones preparados. Todo eso está rindiendo sus primeros frutos y vendrán muchos más, ¡gracias!

Morrolangas, tú también tienes mucho que ver en este asunto desde llevarme al kínder hasta decirme que me cuidara cada vez que salía con mis amigos o me iba a la escuela. Te agradezco que escuches y me aconsejes respecto a cualquier tema por más absurdo que este sea, por las risas, bromas y tonteras que hacemos, ¡gracias por formar parte de esto!

Ana, hermana porque desde hace varios años yo te considero así por todos estos años de amistad y complicidad, tengo muchas cosas por las cuales agradecerte, pero esas claramente ya las sabes, hemos crecido juntas con sus altas y sus bajas como todo en la vida y como decimos “perfectas no somos”. Gracias por aconsejarme, por escuchar mis podcasts cuando algo no anda bien, por el apoyo, las risas, las tonterías y el “ah estas bien tonta” cuando algo no sale como me lo esperaba.

Se que ya cumplimos grandes metas, pero se vienen más, tanto a nivel profesional como personal y es mi de agrado decirle ¡Se logro Señora! no solo somos hermanas amistad sino hermanas de la misma alma mater.

Elvia Lorena Gomez Bravo.

Agradecimientos

A mis padres **Isidro** y **Francisca** que con su apoyo, paciencia y esfuerzo me ayudaron a concluir esta etapa de la vida, ya que ustedes son el motor de mi vida sin ustedes no hubiera podido lograr tantas metas en la vida, no me queda más que agradecer por tanto sacrificio que realizaron de su parte Los AMO nunca olviden eso, seguiremos creciendo como personas.

A mis **hermanos**, que, con su apoyo incondicional, en todo momento y circunstancia me ayudaron a cumplir este sueño.

A mí **esposa** y a mi **hijo** que con su amor y paciencia me ayudaron a cumplir una meta más en mi vida, son la parte más importante de mi vida esa chispa de alegría que me llego en este camino llamado vida.

A nuestra asesora la **L.I Maricela Lara Martínez**. Quién nos brindó su tiempo y apoyo profesional que fue indispensable para poder realizar esta tesis.

A mis amigos de la Facultad por ese apoyo incondicional que me brindaron durante la trayectoria de la Carrera.

Finalmente, y no menos importante a mi compañera **Elvia Lorena** por su paciencia y apoyo en la realización de esta tesis.

Gustavo Duran Cruz.

Índice

Índice de tablas

Índice de imágenes

Introducción

El gradual desarrollo de la tecnología y el uso generalizado de internet en las organizaciones gubernamentales acarrea una dependencia tecnológica para la realización de sus actividades diarias, esto ha hecho que el acceso a los datos e información sea más fácil.

Por lo cual los requerimientos de seguridad son cada vez mayores ya que buscan la protección contra robos de datos, ataques maliciosos mediante virus, ataques de servicios e incluso hackeo a equipos de cómputo y redes de telecomunicaciones. Los ataques pueden ser internos o externos de la organización y buscan tener acceso a la información para modificar, sustraer o borrar datos.

Motivo por el cual los riesgos pueden atraer impactos financieros o reputacionales los cuales pueden ser prevenidos o corregidos con un conjunto bien definido y correcto de políticas y procedimientos de seguridad.

Dichas políticas y procedimientos de seguridad afectan a toda la organización y, como tal, no es solo materia específicamente tecnológica si no que deben tener el soporte y la participación de los usuarios finales, la dirección, el personal de informática y del área legal.

Resumen Capitular

Capítulo 1 Este capítulo se enfocará en conceptos sobre la Seguridad de la Información, así como la implantación de un sistema de gestión de la información.

Capítulo 2 El papel de las normas en la Seguridad de la Información el cual se dará enfoque en la Norma ISO 27001 orientada a una organización gubernamental.

Capítulo 3 Analizaremos y recomendaremos diversas políticas de seguridad para mejorar el control, transportación y manejo de la información, para reducir riesgos de pérdidas o robos de esta. Así mismo el alcance del Sistema de Gestión de la Seguridad de la Información.

Capítulo 4 Definición de roles y responsabilidades dentro de la organización, así como la explicación detallada de lo que realiza cada área, de igual manera se evaluarán los activos con los que cuenta dicha organización.

Capítulo 5 Aplicación de la metodología OCTAVE.

Capítulo 6 Propuesta de selección e implementación de controles de seguridad con base a la ISO 27002.

Capítulo 7 Propuesta para establecer un programa de mejora de seguridad con el modelo PDCA (Planificar-Hacer-Verificar-Actuar) dentro del área de informática del Municipio de Ecatepec de Morelos.

Capítulo 8 Resultados obtenidos.

Objetivo General
Evaluar la perspectiva que se tiene en las organizaciones sobre la cultura de seguridad informática.

Objetivos Específicos
- Conocer el entorno y ámbito tecnológico en el que opera el área de informática.
- Identificar los activos de la información.
- Revisar y adecuar las políticas de Seguridad de la Información.
- Identificar y analizar los riesgos relacionados con la Seguridad de la Información.
- Identificar y evaluar los controles de seguridad actuales de la información establecidos por el área de informática.
- Buscar una posible solución a las amenazas y riesgos encontrados.
- Sensibilizar a empleados de los posibles riesgos hallados en dicho trabajo.

Hipótesis
El manejo y la digitalización de información se ve altamente expuesta a incidentes, esto deriva a la búsqueda de acciones preventivas y correctivas para prevenir contingencias de Seguridad de la Información.

Marco Teórico
El rápido crecimiento de la tecnología constituido por el internet, redes sociales y los sistemas de información en las organizaciones han provocado que el acceso a la información sea más fácil, las personas empiezan a descubrir el valor de la información y la facilidad de tener acceso a dicha información.

Este fácil acceso a la información ha provocado que otros usuarios no autorizados puedan manipular dicha información. Provocando que miles de personas se dediquen a realizar ataques cibernéticos para poder obtener información confidencial, esto para poder cometer actos ilícitos con la cual pueda dañar empresas, gobierno y a las personas.

Motivo por el cual los riesgos pueden tener impactos como la pérdida, modificación o divulgación de información, o pérdida de acceso información. Los cuales pueden ser prevenidos o corregidos con un conjunto bien definido de políticas y procedimientos de seguridad.

En la actualidad es necesario garantizar la Seguridad de la Información ya que se busca la protección contra robo de datos, ataques maliciosos mediante virus, ataques de servicios e incluso hackeo a equipos de cómputo y redes de telecomunicaciones.

Los controles relacionados a la Seguridad de la Información se refieren al conjunto de políticas, procedimientos y mecanismos que garantizan la confidencialidad, integridad y disponibilidad en el procesamiento de datos utilizados por las organizaciones.

Dichas políticas y procedimientos de seguridad afectan a toda la organización y, como tal, no es solo materia específicamente tecnológica si no que deben tener el soporte y la participación de los usuarios finales, el personal de informática y del área legal.

Tomando en cuenta que la información forma parte de los activos más importantes dentro de la organización, es por eso por lo que deben tener controles de seguridad que les permita garantizar que la información contenida en los sistemas informáticos sea confiable, esté disponible y se mantenga íntegra, por lo cual incorporar lineamientos de seguridad en los procesos de riesgo minimiza posibles pérdidas de información o el mal manejo de dicha información.

Marco referencial

A continuación, se explicarán los conceptos que se utilizaran para el desarrollo de la investigación, esto para mostrar los procedimientos que se podrían utilizar para lograr una mejor interpretación de los resultados.

Activo de información: “se puede describir como información o datos que son de valor para la organización, estos pueden existir en forma física (papel, CD u otros medios) o electrónicamente (almacenado en base de datos, en archivos, en computadoras personales)” Norma internacional ISO / IEC 27000, 2018, p. 11)

Activo: “cualquier recurso que tiene valor para la organización” (ISO/IEC, 2013, p. 6)

Amenaza: “se refiere a un posible evento no deseado” (Norma internacional ISO / IEC 27000, 2018, p. 10)

Contenedor de activos de información: es donde los activos de información son almacenados, transportados o procesados es decir el lugar donde “vive”.

Controles de seguridad: “acción o acciones que se utilizan para minimizar riesgos” (Norma internacional ISO / IEC 27000, 2018, p. 20)

Hardware: dispositivos electrónicos que proporcionan capacidad de cálculo, dispositivos de interconexión (por ejemplo, conmutadores de red, dispositivos de telecomunicación) que permiten el flujo de datos y dispositivos electromecánicos (como sensores, motores, bombas) que proporcionan una función externa del mundo real.

Impacto: es el efecto de una amenaza y los objetivos de una organización (Norma internacional ISO / IEC 27000, 2018, p. 21)

Norma ISO 27001: “es una norma internacional que detalla lineamientos de Seguridad de la Información los cuales permiten implementar en la gestión de Seguridad de la Información de cualquier organización, empleando controles para mejorar continuamente la seguridad física y lógica de la información” (ISO/IEC 2005, p.5)

Lo que permite disminuir posibles riesgos en la vulnerabilidad de los sistemas informáticos manipulados por personas que se encuentran dentro y fuera de la organización.

Políticas de Seguridad de la Información: “es aquel documento en donde se delimita y se define las responsabilidades del usuario para la protección de información confidencial, está a su vez supervisa las medidas de seguridad y su efectividad” (ISO/IEC, 2013, p.2)

Riesgo: “es la posibilidad de sufrir daños o pérdidas” (Norma internacional ISO / IEC 27000, 2018, p. 8)

Seguridad de la Información: “establece, implementa, opera, monitorea, revisa, mantiene y mejora la Seguridad de la Información” (ISO/IEC 27001)

Seguridad informática: “es el conjunto de normas y reglas las cuales garantizan la confidencialidad, integridad y disponibilidad de la tecnología abarcando hardware y software” (Baca, 2016, p.12)

Sistema de Gestión de Seguridad de la Información (SGSI): “son aquellos sistemas que implementan controles de seguridad esto para lograr tener un mayor control de la Seguridad de la Información” (Norma internacional ISO/ IEC 27000)

Software: programas de computadora, estructuras de datos y documentación que sirven para hacer efectivo el método, procedimiento o control lógico que se requiere.

Vulnerabilidades: “son los fallos de los sistemas de seguridad” (ISO/IEC, 2013, p.6)

Capítulo 1 Implementación de un Sistema de Gestión de la Seguridad de la Información.

1.1. Definición de información.

Norma Internacional / IEC 27000 (2018) señala que al definir información decimos que es todo conjunto de datos organizados con un contexto específico para una organización independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

1.1.1. Definición de Seguridad de la Información.

Norma Internacional / IEC 27000 (2018), señala que la Seguridad de la Información es aquella que consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.

- Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- Integridad: mantenimiento de la exactitud y completitud de la información.
- Disponibilidad: acceso y utilización de la información por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

1.2. Sistema de Gestión de la Seguridad de la Información.

Norma Internacional / IEC 27000 (2018) refiere a que un SGSI se orienta principalmente en establecer, implementar, operar, monitorear, revisar, mantener y mejorar la Seguridad de la Información de una organización este consiste en: políticas, procesos, procedimientos, estructuras organizativas, software y hardware, teniendo como objetivo la protección de los activos de información. Esto implica identificar qué controles existen y son implementados.

El diseño e implementación del SGSI debe estar adaptado a las necesidades y objetivos de la organización, los requisitos de seguridad, los procesos de negocio y la estructura organizacional y principales marcos normativos cuando estos apliquen.

La correcta implantación de un SGSI permite a una organización:

- Lograr una mayor seguridad en sus activos de información mismos que son protegidos contra amenazas.
- Identificación y evaluación de riesgos de seguridad, seleccionando y aplicando controles midiendo y mejorando su eficacia.
- Lograr efectivamente el cumplimiento legal y regulatorio.

1.2.1. Implantación de un SGSI.

Norma Internacional / IEC 27000 (2018) refiere que para una correcta implantación de un Sistema de Seguridad de la Información dentro de una organización es necesario tomar en cuenta las 10 etapas o fases siguientes:

Etapa 1: definición de las políticas de seguridad y del alcance de SGSI.

El alcance identifica los procesos de negocio, los recursos de la información y tecnológicos, las personas clave y las relaciones con proveedores.

Etapa 2: definición de responsabilidades y asignación de recursos.

Etapa 3: identificación y registro de activos estos pueden ser identificados mediante:

- Necesidades de procesamiento, almacenamiento y comunicación.
- Requisitos legales o marcos normativos.

Etapa 4: análisis y gestión de riesgos.

Esta debe identificar, cuantificar y priorizar los riesgos con base a criticidad de aceptación previamente establecida por la organización misma que deberá actualizarse periódicamente para notar posibles cambios en los activos de información, amenazas, vulnerabilidades e impactos en la Seguridad de la Información.

Etapa 5: selección e implantación de controles de seguridad.

Es necesario contemplar que para un buen funcionamiento del SGSI la organización deberá monitorear y evaluar su desempeño frente a las políticas y objetivos de esta. En la evaluación se verifica que los controles son adecuados para el tratamiento de los riesgos delimitados por el alcance del SGSI y con esta información se establece las acciones correctivas, preventivas y de mejora.

El empleo de controles debe garantizar la reducción de riesgos a un nivel aceptable los cuales contemplan los requisitos y limitaciones legales, objetivos organizacionales, requisitos y limitaciones operacionales, costo de implementación y operaciones. Así cada organización debe definir los criterios para determinar si estos pueden ser aceptados o no.

Etapa 6: establecer un programa de mejora de la seguridad.

Para una correcta implementación y correcto funcionamiento es necesario la creación de un plan de mejora continua el cual busca lograr preservar la confidencialidad, disponibilidad e integridad de la información.

Algunas de las acciones de mejora incluyen:

- Análisis y evaluación para identificar las áreas de mejora.
- Establecer objetivos de mejora.
- Busca las posibles soluciones para alcanzar los objetivos.
- Implementar la solución seleccionada.

- Medir, verificar, analizar y evaluar los resultados de la implementación.
- Formalización de cambios.

Etapa 7: completar la documentación del SGSI.
Etapa 8: revisión y auditoría interna del proyecto de implantación del SGSI.
Etapa 9: realización de la auditoría de certificación.
Etapa 10: ejecutar las recomendaciones de la auditoría.

La implementación exitosa del SGSI se ve influenciada por factores críticos de éxito los cuales pueden ser:

- Políticas, objetivos y actividades de Seguridad de la Información alineados con los objetivos.
- Un enfoque y un marco para diseñar, implementar, monitorear, mantener y mejorar la Seguridad de la Información consistente con la cultura organizacional.
- Apoyo y compromiso visibles de todos los niveles de gestión, especialmente de la alta dirección.
- Un programa eficaz de concientización, capacitación y educación sobre Seguridad de la Información, que informe a todos los empleados y otras partes relevantes de sus obligaciones establecidas en las políticas de Seguridad de la Información.
- Un proceso eficaz de gestión de incidentes de Seguridad de la Información.
- Un sistema de medición para evaluar el desempeño en la gestión de Seguridad de la Información.

Algunos de los beneficios de la implementación de un SGSI es la reducción en los riesgos de Seguridad de la Información (es decir la reducción de la probabilidad y/o el impacto causado por incidentes de Seguridad de la Información).

1.2.2. Conformación de un Sistema de Gestión de la Seguridad de la Información.
Un Sistema de Gestión de Seguridad de la Información debe estar formado por:

- Alcance del SGSI: el cual dice que en este ámbito la organización queda sometida al SGSI delimitando las áreas, roles y responsabilidades.
- Políticas y objetivos de seguridad: este es un documento en el cual se establece el compromiso de la dirección y el enfoque de la organización en la gestión de la Seguridad de la Información.
- Procedimientos y mecanismos de control que soportan al SGSI: son aquellos procedimientos que regulan el propio funcionamiento del SGSI.
- Enfoque de evaluación de riesgos: la cual es la descripción de la metodología a emplear esta describe el cómo se realizará la evaluación de las amenazas, vulnerabilidades e impactos en relación con los activos de información contenidos dentro del alcance desarrollando criterios de aceptación de riesgo y fijación de niveles de riesgo aceptables.
- Informe de evaluación de riesgos: este es un estudio resultante de aplicar la metodología de evaluación de riesgos a los activos de información de la organización.

- Plan de tratamiento de riesgos: el cual se realiza un documento que identifica las acciones de la dirección, los recursos, las responsabilidades y las prioridades para gestionar los riesgos de Seguridad de la Información, en con ayuda de las conclusiones obtenidas de la evaluación de riesgos.
- Procedimientos documentados: estos deben de estar documentados para asegurar la planificación, operación y control de los procesos de Seguridad de la Información, así como para medir la eficacia de los controles implantados.
- Declaración de aplicabilidad: este documento contiene los objetivos de control y los controles contemplados por el SGSI, basado en los resultados de los procesos de evaluación y tratamiento de riesgos.

1.2.3. Alcance del SGSI para el área de informática.

Recomendaremos diversas políticas, controles y medidas de seguridad para lograr un correcto manejo, control y transportación de la información, buscando así la modificación, robo o pérdida dentro del área de informática.

Algunas de estas políticas buscaran:

- Reducción de robo y pérdida de información.
- Sensibilizar a directivos y capital humano sobre las posibles amenazas a las que se enfrentan, teniendo así una cultura de Seguridad de la Información
- Controles para accesos físicos y lógicos.
- Delimitación correcta de roles y responsabilidades.
- Evitar duplicidad de información.

Cabe mencionar que dentro del municipio sólo están establecidas algunas políticas y no existen sanciones por incumplimiento, también la documentación se encuentra desactualizada.

Capítulo 2 Aplicación de estándar ISO 27001 a una organización gubernamental.

2.1. ¿Qué son las ISO?

ISOTools. (21 febrero 2019). Las Normas ISO son un conjunto de Normas orientadas a ordenar la gestión de una organización en sus distintos ámbitos. Las Normas ISO son establecidas por el Organismo Internacional de Estandarización (ISO), y se componen de estándares y guías relacionados con sistemas y herramientas específicas de gestión aplicables en cualquier tipo de organización.

Estas se crearon con la finalidad de ofrecer orientación, coordinación, simplificación y unificación de criterios a las empresas y organizaciones con el objeto de reducir costes y aumentar la efectividad, así como estandarizar las normas de productos y servicios para las organizaciones internacionales. Estas buscan homogeneizar las características y los parámetros de calidad y seguridad de los productos y servicios.

2.1.1. Norma ISO/IEC 27000 e ISO 27001.

ISO/IEC (2013) señala que tanto la Norma ISO/IEC 27000 como la Norma ISO/IEC 27001 son un conjunto de estándares internacionales relacionadas a Seguridad de la Información las cuales fueron creadas para la implementación de un Sistema de Gestión de la Seguridad de la Información que considera el análisis, la gestión de los riesgos de TIC y aplicación de controles que garanticen la confidencialidad, integridad y disponibilidad de los activos de información.

Estas normas también van dirigidas a los activos de la información, los cuales son necesarios para los sistemas de Seguridad de la Información.

Costas (2010) señala que dichos activos tienen diferentes características en materia seguridad, confidencialidad, integridad, disponibilidad.

- Autentificación: propiedad que permite identificar al generador de la información. Por ejemplo, al recibir un mensaje de alguien, estar seguro de que es de ese alguien el que lo ha mandado, y no una tercera persona haciéndose pasar por la otra (suplantación de identidad). En un sistema informático se suele conseguir este factor con el uso de cuentas de usuario y contraseñas de acceso.
- Confidencialidad: propiedad de que la información no esté disponible o se revela a personas, entidades o procesos no autorizados.
- Integridad: protege la modificación o destrucción no autorizada de los activos.
- Disponibilidad: propiedad de proteger la exactitud y completitud de los activos.

2.1.2. Las normas ISO dentro de instituciones del sector gubernamental.

CTMA CONSULTORES. (2020). En la actualidad el gobierno se enfrenta al constante avance tecnológico esto ocasiona que se enfrente a muchos riesgos y amenazas. Sobre todo, en la última década, ya que a este periodo de tiempo se le denominó como la era de la información.

A este periodo de tiempo se le puede caracterizar por el aumento de información disponible, la posibilidad de acceso a dicha información por un gran número de personas desde múltiples ubicaciones y una mayor velocidad en procesamiento y almacenamiento de la información.

El acceso a la información desde diferentes ubicaciones se realiza mediante las redes de comunicaciones. Hoy en día las entidades de gobierno utilizan los servicios como son los servicios de correo electrónico, el acceso a sitios web para búsqueda de información, hacer transacciones, etc. Todo lo anterior obliga a prestar especial atención al modo de operar a través de las redes, estos deberán ser utilizados con las debidas medidas de seguridad y control.

Esta información adquiere diferentes formas y es tratada, almacenada y presentada a diferentes niveles de la organización.

Laudon y Laudon, (2006). Estas necesidades de información, su tratamiento y aplicación conforman los Sistemas de Información (SI). Un Sistema de Información puede definirse como un conjunto de componentes interrelacionados que permiten capturar, procesar, almacenar y distribuir información para apoyar la toma de decisiones y el control de una institución.

Algunos elementos o componentes que podemos identificar en los SI pueden ser los activos de información los cuales son: personas, hardware, bases de datos, documentación, software, etc.

Estos elementos, van a estar presentes en todas las situaciones y como en el caso que nos ocupa queremos centrarnos en la Seguridad de la Información, veremos que no podemos abordarla de forma independiente, sino dentro del marco definido por las relaciones entre la información y los otros componentes del Sistema de Información en el marco de la gestión.

Fernández y Piattini, (2012). En el año 1992, el Consejo de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) adoptó una importante Recomendación para la seguridad de los sistemas de información, en la que encontramos que:

“La seguridad de los Sistemas de Información tiene por objetivo proteger los intereses de los que cuentan con Sistemas de Información contra los perjuicios imputables a defectos de disponibilidad, de confidencialidad y de integridad” (Fernández y Piattini,2012).

Es por eso por lo que las entidades de gobierno se han apegado a la Norma ISO/IEC 27000 ya que esta Norma establece la implementación de la Seguridad de la Información no solo empresarial sino también se adecua a las entidades de gobierno.

Los requisitos de la Norma 27001 aporta un Sistema de Gestión de la Seguridad de la Información (SGSI) la cual consiste en medidas orientadas a proteger la información contra cualquier amenaza de forma que garanticemos en todo momento las actividades.

2.1.3. Sistemas de Gestión de la Seguridad de la Información de acuerdo con la Norma ISO/IEC 27001.

ISO/IEC (2013). Esta Norma ha definido los requisitos para poder establecer, implementar, operar, supervisar, revisar, mantener y mejorar un SGSI, documentado los posibles riesgos que puede tener el gobierno ya que ellos son los encargados de manipular información muy valiosa como puede ser financiera e información personal de la población entre otras.

La Gestión de la Seguridad de la Información implica la planificación, organización, dirección y control de los recursos (humanos, financieros, materiales, tecnológicos, etc.), con el fin de mejorar la Seguridad de la Información.

2.1. Modelo PHVA (Planificar, Hacer, Verificar, Actuar).

ISOTOOLS. (2015). Estas Normas están basadas en los procesos que utiliza el modelo PHVA (Planificar, Hacer, Verificar, Actuar). En cada una de las fases se realizan una serie de acciones generales esta genera una serie de documentación y registros como se muestra a continuación.

Tabla 1: modelo PHVA.

Fase	Actividad	Documento / Registro
Planificar	Definición de la política, alcance y objetivos del SGSI. Estructura organizacional. Gestión del riesgo (análisis, estimación, aceptación,evaluación). Aprobación del sistema.	Política, alcance y objetivos del SGSI. Procedimientos de soporte del SGSI (documentación, auditoría interna, acciones de mejora). Metodología de evaluación de riesgos. Informe de evaluación de riesgos Declaración de aplicabilidad.
Hacer	Implementación de la política y los controles. Acciones formativas. Diseño del modo de medir la eficacia y de gestionar las incidencias.	Plan de tratamiento del riesgo. Procedimientos específicos de operación del SGSI y de medición de la eficacia de los controles.

Fase	Actividad	Documento / Registro
Verificar	Ejecución de procedimientosde revisión y de medición de la eficacia de los controles. Gestión de incidencias. Auditoría interna. Revisión del sistema.	Registros asociados. Informes de auditoría interna y de revisión por la dirección.
Actuar	Objetivos de mejora. Acciones preventivas y correctivas.	Registros asociados

Fuente: elaboración propia.

Capítulo 3 Definición de Políticas de Seguridad y del Alcance del Sistema de Gestión de la Seguridad de la Información.

3.1. Políticas de Seguridad.

Gómez, A. (2006) define como políticas a aquellas definen qué se debe proteger dentro del sistema (activos o recursos), mientras que los procedimientos de seguridad describen cómo se debe conseguir dicha protección a través de tareas y estas a su vez pueden generar evidencia de incidentes de seguridad que facilitan el seguimiento, control y supervisión del funcionamiento del sistema de gestión de la Seguridad de la Información (p.71).

El objetivo de una política es concientizar a todo aquel que esté involucrado con la seguridad de la información y de sus activos ya sea personal interno de la organización o terceros. Por lo tanto, una política deberá redactarse de forma que pueda ser comprendida por todo el personal y deberá ser comunicada por los canales de comunicación establecidos por la organización.

3.1.1. Objetivos de las políticas de seguridad.

Gómez, A. (2006) señala que una Política de Seguridad contendrá los objetivos de la organización en materia de seguridad del Sistema de Información, generalmente englobados en cuatro grupos:

- Identificar las necesidades de seguridad y los riesgos que amenazan al sistema de información, así como evaluar los impactos ante un eventual ataque.
- Relacionar todas las medidas de seguridad que deben implementarse para afrontar los riesgos de cada activo o grupo de activos.
- Proporcionar una perspectiva general de las reglas y los procedimientos que deben aplicarse para afrontar los riesgos identificados en las diferentes áreas de la organización.
- Detectar todas las vulnerabilidades del sistema de información y controlar los fallos que se producen en los activos, incluidas las aplicaciones instaladas.
- Definir un plan de contingencias.

3.1.2. Características de las Políticas de Seguridad.

Gómez, A. (2006) define que las Políticas de Seguridad de una organización deberán de cumplir con las siguientes características y requisitos (p.73, p.74.):

- Deberán de ser implementadas a través de determinados procedimientos administrativos y la publicación de unas guías de uso aceptable del sistema por parte del personal, así como mediante la instalación, configuración y mantenimiento de determinados dispositivos y herramientas hardware y software que implanten servicios de seguridad.
- Definir claramente las responsabilidades exigidas al personal con acceso al sistema: técnicos, analistas y programadores, usuarios finales, directivos, personal externo a la organización.

- Deben cumplir con las exigencias del entorno legal (protección de datos personales, protección de la propiedad intelectual, código penal).
- Se tienen que revisar de forma periódica para poder adaptarlas a las nuevas exigencias de la organización y del entorno tecnológico y legal. En este sentido, se debería contemplar un procedimiento para garantizar la revisión y actualización periódica de las Políticas de Seguridad.
- Las políticas de seguridad no deben limitarse a cumplir con los requisitos impuestos por el entorno legal o las exigencias de terceros, sino que deberían estar adaptadas a las necesidades reales de cada organización.

Por otra parte, al definir las políticas se deben tomar en cuenta las vulnerabilidades la cual se puede definir como cualquier debilidad en un sistema informático que pueda permitir a las amenazas producir daños o pérdidas a la organización. Estas pueden estar ligadas a procedimientos mal definidos o sin actualizar, ausencia de políticas o políticas no actualizadas, factor humano es decir falta de sensibilización con acceso al sistema, manejo de información, etc.

3.1.3. Definición e implantación de las políticas.

Gómez, A. (2006) menciona que a la hora de definir y crear las Políticas de Seguridad dentro de una organización se debe contemplar lo siguiente (p. 77):

- Alcance: recursos, instalaciones y procesos de la organización sobre los que se aplican.
- Objetivos perseguidos y prioridades de seguridad.
- Compromiso de la dirección de la organización.
- Clasificación de la información e identificación de los activos a proteger.
- Análisis y gestión de riesgos.
- Elementos y agentes involucrados en la implantación de las medidas de seguridad.
- Asignación de responsabilidades en los distintos niveles.
- Definición clara y precisa de los comportamientos exigidos y de los que están prohibidos por parte del personal.
- Identificación de las medidas, normas y procedimientos de seguridad a implantar.
- Gestión de las relaciones con terceros (clientes, proveedores).
- Gestión de incidentes.
- Planes de contingencia y de continuidad del negocio.
- Cumplimiento de la legislación del negocio.
- Definición de las posibles violaciones y las consecuencias derivadas del incumplimiento de las políticas de seguridad.

De esta manera, podemos señalar cuales son los distintos participantes que deberían estar implicados en la definición de las Políticas de Seguridad dentro una organización:

- Directivos y responsables de los distintos departamentos y áreas funcionales de la organización.
- Representantes de los usuarios que pueden verse afectados por las medidas adoptadas.
- Consultores externos expertos en seguridad.

El acceso a la documentación debe ser clara y detallada sobre todas las medidas y directrices de seguridad, así como los planes de formación y sensibilización inicial de los nuevos empleados que se incorporan a la organización son otros dos aspectos de vital importancia. La documentación debería incluir contenidos sencillos y accesibles para personal no técnico, incorporando un glosario con la terminología técnica empleada en los distintos apartados.

En cada documento se podría incluir la siguiente información:

- Título y ID.
- Fecha de publicación.
- Fecha de entrada en vigor.
- Fecha prevista de revisión o actualización.
- Ámbito de aplicación (a toda la organización o solo a una determinada área).
- Descripción detallada (redactada de forma comprensible para todos los empleados) de los objetivos de seguridad.
- Personal responsable de la revisión y aprobación.
- Documento (o documentos) al que reemplaza o modifica.
- Otros documentos relacionados.

En los procedimientos de seguridad será necesario especificar además otra información adicional:

- Descripción detallada de las actividades que se deben ejecutar.
- Personas o departamentos responsables de su ejecución.
- Momento y/o lugar en que deben realizarse.
- Controles para su correcta ejecución.

3.2. Políticas existentes dentro del área de Informática.

Dentro del área de informática se cuenta con algunas políticas y restricciones, pero estas no cuentan con sanciones en caso de incumplimiento.

Restricciones actuales:

- Uso de Wifi requiere de una previa autorización.
- Uso de redes sociales son bloqueadas por parte de un externo o controles de red.
- Uso de claves para acceso a información sensible.

Vulnerabilidades

- Políticas no establecidas u obsoletas.
- Sanciones no establecidas.
- No se evalúan riesgos y amenazas que se presentan.
- Documentación no actualizada.

3.2.1. Política para la Seguridad de la Información.
La información debe ser protegida por los usuarios que tengan acceso y procesamiento. El acceso a esta debe ser mediante el uso de claves y estas no deben ser compartidas entre miembros del área.

Vulnerabilidades

- Préstamo de claves de acceso.
- Acceso de cualquier persona a los equipos de cómputo.

3.2.2. Política Uso de Dispositivos Móviles.
Se darán las condiciones adecuadas para el manejo de dispositivos móviles o gadgets que hagan uso de la infraestructura y servicios del municipio.

Vulnerabilidades

- Mal uso del celular ya que deriva a una pérdida de tiempo en horas de trabajo.
- Afectación del rendimiento de los empleados.

3.2.3. Política de Gestión de Riesgos.
Esta es llevada a cabo a través de una adecuada definición y asignación de funciones y responsabilidades. Así mismo llevar a cabo análisis de riesgos, ya sea de tipo tecnológicos, ambientales o de ubicación. Su evaluación consta de las siguientes etapas:

- Identificación de amenazas y vulnerabilidades sobre los activos de información.
- Identificación de riesgos y evaluación de riesgos.
- Monitoreo.

Vulnerabilidades

- No se realiza una evaluación de los riesgos y amenazas.
- No hay un control o medidas contra las amenazas encontradas.
- No hay interés por parte de los directivos.

3.2.4. Política Gestión de Activos de la Información.
Toda la información y procesos manejados dentro del área de informática, así como los activos donde estos se almacena y/o procesa deben ser manejados por medio de:

- Un grado de confidencialidad.
- Acceso por medio de claves.
- Fijar un responsable por la información solicitada.

Vulnerabilidades

- Préstamo de claves de acceso.

3.2.5. Política de Control de Acceso.

Se debe establecer medidas de seguridad para el acceso físico a las instalaciones, mantener actualizado el acceso lógico para la red, sistemas operativos, bases de datos y aplicaciones, estos deberán ser respaldados por una cultura de seguridad por parte del municipio y empleados.

Se establecerá un acceso limitado a la información a los usuarios activos, dependiendo su rol y responsabilidad esto permitirá dar seguimiento sobre cadauno de estos.

Para el acceso a los servicios o información, el jefe de cada departamento deberá realizar una solicitud a el encargado de informática, especificando los datos exactos del usuario (nombre, área y puesto) y servicios a los que tendrá acceso.

Vulnerabilidades

- Préstamos entre los empleados de claves de acceso.
- Las medidas de control de acceso no están actualizadas.
- Los jefes de cada departamento no tienen un control de las solicitudes.

3.2.6. Política de Manejo de Internet.

El uso de internet debe estar limitado para asuntos laborales. Si se requiere uso de wifi dentro de un departamento este deberá solicitarlo al área de telefonía.

Vulnerabilidades

- Acceso a redes sociales

Algunas restricciones con las que cuenta son:

- El uso del wifi será mediante claves previamente solicitadas.
- El acceso a redes sociales es bloqueado a través de un servicio de un tercero.
- El acceso a la información es mediante el uso de accesos y privilegios en cada nivel.

3.3. Posibles solucionesa políticas inexistentes y vulnerabilidades encontradas.

Se propondrá mejoras a las políticas existentes para buscar una solución a las vulnerabilidades encontradas y sugerir políticas en caso de que no existan dentro del área de informática.

La adopción de nuevas políticas contempla los siguientes aspectos:

- Alcance: recursos, instalaciones y procesos de la organización sobre los que se aplican.
- Objetivos.
- Compromiso de la Dirección.
- Clasificación de la información e identificación de los activos a proteger.

- Análisis y gestión de riesgos.
- Elementos involucrados para la implantación de las medidas de seguridad.
- Identificación de roles y funciones.
- Identificación de las medidas, normas y procedimientos de seguridad a implantar.
- Gestión de relaciones con terceros.
- Definición de las posibles violaciones y de las consecuencias derivadas del incumplimiento de las Políticas de Seguridad.

3.3.1. Política de Infraestructura.

El municipio de Ecatepec de Morelos deberá considerar los estándares vigentes de cableado estructurado durante el diseño de nuevas áreas o en el crecimiento de las áreas existentes.

3.3.2. Política Instalación de Equipo de Cómputo.

La instalación del equipo de cómputo quedará sujeto a los siguientes lineamientos:

- Los equipos para el uso interno se instalarán en lugares adecuados, protegidos del polvo y tráfico de personas.
- El área de informática, así como las áreas operativas deberán contar con un plano actualizado de las instalaciones eléctricas y de comunicaciones del equipo de cómputo.
- Las instalaciones eléctricas y de comunicaciones, estarán preferiblemente fijas o en su defecto resguardadas del paso de personas o materiales, y libres de cualquier interferencia eléctrica o magnética.
- Las instalaciones se apegan estrictamente a los requerimientos de los equipos, cuidando las especificaciones del cableado y de los circuitos de protección necesarios.
- En ningún caso se permitirán instalaciones improvisadas o sobrecargadas.
- La supervisión y control de las instalaciones se llevará a cabo en los plazos y mediante los mecanismos que establezca el equipo.

3.3.3. Política de Controles.

Se debe llevar a cabo un control total y sistematizado de los recursos de cómputo y lineamiento.

El encargado del área de informática será el responsable de organizar al personal encargado del mantenimiento preventivo y correctivo de los equipos de cómputo.

3.3.4. Política Respaldo de Información.

Las bases de datos serán respaldadas periódicamente en forma automática o manual.

Las bases de datos deberán tener una réplica en uno o más equipos remotos alojados en un lugar seguro.

Los demás respaldos (una copia completa) deberán ser almacenados en un lugar seguro y apartado del sitio de trabajo, en bodegas con los estándares de calidad para almacenamiento de medios magnéticos.

Para reforzar la Seguridad de la Información, los usuarios, bajo su criterio, deberán hacer respaldos de la información en sus discos duros frecuentemente, dependiendo la importancia y frecuencia de cambio.

3.3.5. Política Seguridad de la Información.

La información manejada en la organización es utilizada para fines de servicios públicos, como por ejemplo pago de predial, agua, etc. La información proporcionada no deberá ser dañada, modificada o robada ya que es información sensible y se lleva a cabo un incumplimiento el municipio tomará acciones legales.

Se tomarán en cuenta los siguientes lineamientos:

- El tratamiento de la información y documentación estratégica y confidencial estará bajo el resguardo del director de cada área, quien determinará los criterios para tener acceso a dicha información, así como para seleccionar al personal que tendrá acceso y autorización para su uso.
- El personal responsable deberá asegurar el manejo y la integridad de la información que reside en medios electrónicos y/o en documentos.
- Todo documento referido a procesos, instrucciones y/o formatos serán considerados propiedad del Municipio de Ecatepec de Morelos, por lo que queda prohibida su reproducción no autorizada.
- Toda la información contenida en la página web del municipio, así como cuentas en diferentes redes sociales, es de carácter público y queda prohibido el uso indebido de ella.
- Todos los contratos en los que participa el Municipio de Ecatepec de Morelos deben incluir una cláusula de confidencialidad.
- El Municipio de Ecatepec de Morelos sólo puede realizar intercambios de información de datos personales de sus colaboradores o de candidatos, exclusivamente con bolsas de trabajo para propósitos de reclutamiento y con su consentimiento explícito.
- Todos los procesos, tecnologías e investigaciones realizadas dentro de la organización por parte del personal serán propiedad del Municipio de Ecatepec de Morelos.
- El uso de documentos oficiales será única y exclusivamente para fines públicos y/o empresariales.

3.3.6. Política de Uso de Periféricos y Medios de Almacenamiento.

Los dispositivos de almacenamiento de uso externo comprenden las unidades que se pueden conectar como una memoria USB, por medio de un cable de datos, mediante una conexión inalámbrica directa a cualquier equipo de cómputo. Entre estos se pueden encontrar, pero no se limita a:

- Memorias Flash USB
- IPhone/Smartphones
- SD Cards/Mini SD Cards/Micro SD Cards
- PDAS/ Tabletas
- Dispositivos con tecnología Bluetooth
- Tarjetas Compact Flash

- Discos duros externos

Se tomarán en cuenta los siguientes lineamientos:

- Establecimiento de reglas que permitan controlar el acceso de aplicaciones y/o dispositivos a los recursos del sistema, con el fin de prevenir riesgos de infección y/o seguridad; no se bloqueara el acceso a dispositivos como CD/DVD-ROM o discos externos.
- Los usuarios cuyos equipos computacionales están equipados con grabadores para CD, DVD o ambos utilizaran estos dispositivos exclusivamente para archivos de respaldo de documentos originales, base de datos o copias de software autorizadas.
- El uso indebido de estos dispositivos para copias no autorizadas por el autor ("piratas") de cualquier programa del equipo o software es responsabilidad del usuario bajo cuyo resguardo esté el equipo computacional.
- Bloqueo a ejecución de aplicaciones desde CD-ROM/DVD-ROM y dispositivos de almacenamiento removibles incluyendo Autorun.inf.

3.3.7. Política Administración de Redes.

Las redes tienen como propósito principal servir en la transformación e intercambio de información dentro del Municipio de Ecatepec de Morelos entre usuarios, departamentos, oficinas y hacia afuera a través de conexiones con otras redes.

El departamento de informática no es responsable por el contenido de datos ni por el tráfico que en ella circule, la responsabilidad recae directamente sobre el usuario que los genere o solicite.

Se tomarán en cuenta los siguientes lineamientos:

- Nadie puede ver, copiar, alterar o destruir la información que reside en los equipos sin el consentimiento explícito del responsable del equipo.
- No se permite el uso de los servicios de la red cuando no cumplan con las labores del Municipio de Ecatepec de Morelos.
- Las cuentas de ingreso a los sistemas y los recursos de cómputo son propiedad del Municipio de Ecatepec de Morelos
- Todas las cuentas de acceso a los sistemas y recursos son personales e intransferibles.
- Cuando se detecte un uso incorrecto, se cancelará la cuenta o se desconectará temporal o permanentemente al usuario o red involucrada dependiendo de las políticas. La reconexión se hará en cuanto se considere que el uso no aceptable se ha suspendido.

3.3.8. Política de Servidores.

La responsabilidad de verificar la instalación, configuración e implementación de seguridad, en los servidores conectados a la Red.

Durante la configuración de los servidores deben generar las normas para el uso de los recursos del sistema y de la red, principalmente la restricción de directorios, permisos y programas a ser ejecutados por los usuarios.

Los servidores que proporcionen servicios a través de la red e internet deberán:

- Funcionar las 24 horas del día los 365 días del año.
- Recibir mantenimiento preventivo mínimo una vez al año.
- Recibir mantenimiento semestral que incluya depuración de logs.
- Recibir mantenimiento anual que incluya la revisión de su configuración.

La información de los servidores deberá ser respalda de acuerdo con los siguientes criterios, como mínimo:

- Diariamente, información crítica.
- Semanalmente, los documentos web.
- Mensualmente, configuración del servidor y logs.

Tener el apoyo por medios magnéticos o en forma documental, de las operaciones necesarias para reconstruir los archivos dañados.
Contar con un instructivo de operación para la detección de posibles fallas, para que toda acción correctiva se efectúe con la mínima degradación posible de los datos.
Contar con un directorio del personal interno y del personal externo de soporte, al cual se pueda recurrir en el momento en que se detecte cualquier anomalía.
Ejecutar pruebas de la funcionalidad del plan.
Mantener revisiones del plan a fin de efectuar las actualizaciones respectivas.

3.3.9. Política uso de Software.

Los empleados con funciones y responsabilidades para con el software institucional deben seguir los siguientes lineamientos para proteger este activo y la información que a través de él se maneje.

Los usuarios del servicio de Internet deben evitar la descarga de software desde internet, así como su instalación en las estaciones de trabajo o dispositivos móviles asignados para el desempeño de sus labores.

3.3.10. Administración de Software.

Se debe contar en todo momento con inventario actualizado del software de su propiedad, el comprado a terceros o desarrollando internamente, el adquirido bajo licenciamiento, el entregado y el recibido. Las licencias se almacenan bajo los adecuados niveles de seguridad e incluidas en un sistema de administración, efectuando continuos muestreos para garantizar la consistencia de la información allí almacenada.

Los ambientes de desarrollo de sistemas, pruebas y producción deben permanecer separados para su adecuada administración, operación, control y seguridad. Los programas que se encuentren en el ambiente de desarrollo se modificarán únicamente por el personal autorizado, se considerarán planes de contingencia y recuperación.

3.3.11. Adquisición de Software.

El software contará con acceso controlado que permita al propietario del recurso restringir el acceso al mismo. El software protegerá los activos que estén en riesgo de aquellos usuarios que puedan acceder a ellos sin los debidos permisos.

Cada usuario se identificará por medio de un único código de identificación de usuario y clave, antes de que se le permita el acceso al sistema.

3.3.12. Política Uso de Hardware.

Los equipos de cómputo no deben ser alterados ni mejorados (cambios del procesador, memoria o tarjetas) sin el consentimiento, evaluación técnica y autorización del área responsable (Informática).

Los funcionarios deben reportar a los entes pertinentes sobre daños y pérdida del equipo que tengan a su cuidado y sea propiedad del Municipio de Ecatepec de Morelos. La intervención directa para reparar el equipo debe estar expresamente prohibida. Los encargados de informática deben proporcionar personal interno o externo para la solución del problema reportado.
Todos los equipos deben estar relacionados en un inventario que incluya la información de sus características, configuración y ubicación.

Todo hardware que adquiera el Municipio de Ecatepec de Morelos debe conseguirse a través de canales de compra estándares.

Para todos los equipos y sistemas de comunicación utilizados en procesos de producción en la entidad, se debe aplicar un procedimiento formal de control de cambios que garantice que sólo se realicen los cambios autorizados. Este procedimiento de control de cambios debe incluir la documentación del proceso con las respectivas propuestas revisadas, la aprobación de las áreas correspondientes y la manera como el cambio fue realizado.

Todos los productos de hardware deben ser registrados por proveedor y contar con el respectivo contrato de mantenimiento.

Los equipos computacionales, sean estos PC, servidores, LAN, etc. no deben moverse o reubicarse sin la aprobación previa del Administrador o jefe del área involucrada.

3.3.13. Política Uso de Internet.

El área de informática será consciente de la importancia de Internet como una herramienta para el desempeño de labores, proporcionará los recursos necesarios para asegurar su disponibilidad a los usuarios que así lo requieran para el desarrollo de sus actividades diarias.

Se deberá proporcionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de Internet, bajo las restricciones de los perfiles de acceso establecidos.

Se deberá diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de Internet en caso de contingencia interna.

Será necesario monitorear continuamente el canal o canales del servicio de Internet.

Se deberá establecer procedimientos e implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de Internet y evitar el acceso a sitios catalogados como restringidos.

El área será la encargada de generar registros de la navegación y los accesos de los usuarios a Internet, así como establecer e implantar procedimientos de monitoreo sobre la utilización del servicio de Internet.

3.3.14. Política Seguridad Física.

El Municipio de Ecatepec de Morelos tendrá un área que servirá como centro de telecomunicaciones donde ubicaran los sistemas de telecomunicaciones y servidores.

Todos los sistemas de comunicaciones estarán debidamente protegidos con la infraestructura apropiada de manera que el usuario no tenga acceso físico directo.

El acceso de terceras personas debe ser identificado plenamente, controlado y vigilado durante el acceso.

Las visitas internas o externas podrán acceder a las áreas restringidas siempre y cuando se encuentren acompañadas cuando menos por un responsable del área de informática

Las visitas a las instalaciones físicas de los centros de telecomunicaciones se harán en el horario establecido.

El personal autorizado para mover, cambiar o extraer equipo de cómputo es el poseedor de este o el superior responsable, a través de formatos de autorización de Entrada/Salida.

3.3.15. Política de Gestión de Incidentes.

Se describirán las medidas y procedimientos de detección, neutralización y recuperación ante cualquier eventualidad que pueda paralizar total o parcialmente la actividad informática o degraden su funcionamiento, minimizando el impacto negativo de estas sobre la entidad.

Se define como incidente de seguridad a cualquier evento que se produzca, de forma accidental o intencional, que afecte o ponga en peligro las tecnologías de información o los procesos que con ellas se realizan. Incluyen entre otros:

- Acceso (intentos de acceso) no autorizado a un sistema de datos.
- Interrupción no deseada o denegación de servicio.
- Uso no autorizado de un sistema para el procesamiento o almacenamiento de la información.

- Suplantación de identidad.
- Cambios a las características del equipamiento, aplicaciones o datos del sistema sin el consentimiento del responsable de dicho sistema.

Se deberá llevar a cabo procedimientos para evaluar y gestionar los incidentes de la siguiente manera:

- Una correcta evaluación de lo ocurrido.
- A quien, como y cuando debe ser reportado.
- Aspectos relacionados con la documentación pertinente, la preservación de las evidencias y las acciones a seguir.
- Se habilitará un registro donde se consignarán los incidentes que se produzcan, será utilizado como criterio de medición para la gestión del sistema de seguridad informática.

3.3.16. Política Uso Apropiado de Recursos.

Los Recursos Informáticos, Datos, Software, Red y Sistemas de Comunicación están disponibles exclusivamente para cumplir las obligaciones y propósito para la que fueron diseñados e implantados. Todo el personal usuario de dichos recursos debe saber que tiene el derecho de confidencialidad en su uso.

Queda prohibido:

- El uso de estos recursos para actividades no relacionadas con el propósito del municipio, o bien con la extralimitación en su uso.
- Las actividades, equipos o aplicaciones que no estén directamente especificados como parte del Software o de los Estándares de los Recursos Informáticos propios.
- Introducir en los Sistemas de Información o la Red Corporativa contenidos obscenos, amenazadores, inmorales u ofensivos.
- Introducir voluntariamente programas, virus, macros, applets o cualquier otro dispositivo lógico o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración o daño en los Recursos Informáticos.
- Intentar destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos.
- Albergar datos de carácter personal en las unidades locales de disco de los computadores de trabajo.
- Cualquier fichero introducido en la Red o en el puesto de trabajo del usuario a través de soportes automatizados, internet, correo electrónico o cualquier otro medio, deberá cumplir los requisitos establecidos en estas Políticas y, en especial, las referidas a propiedad intelectual y control de virus.

3.3.17. Normas dirigidas a TODOS LOS USUARIOS.

Los usuarios con servicio de Internet deben hacer uso de este en relación con las actividades laborales que así lo requieran.

Los usuarios deben evitar la descarga de software desde internet, así como su

instalación en las estaciones de trabajo o dispositivos móviles asignados para el desempeño de sus labores.

No está permitido el acceso a páginas relacionadas con pornografía, drogas, alcohol, web proxys, hacking y/o cualquier otra página que vaya en contra de la ética.

Los usuarios del servicio de internet tienen prohibido el acceso y el uso de redes sociales tales Facebook, Twitter y otros similares.

No está permitido la descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros.

La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en Internet debe ser autorizada por el jefe respectivo, o a quienes ellos deleguen de forma explícita para esta función, asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.

No está permitido el intercambio no autorizado de información de propiedad del municipio y/o de sus funcionarios, con terceros.

3.3.18. Sanciones.

Las sanciones pueden ser desde una llamada de atención o informar al usuario hasta la suspensión del servicio dependiendo de la gravedad de la falta.

Corresponderá al área de informática hacer las propuestas finales sobre las sanciones a quienes violen las disposiciones en materia de informática.

En cuanto a los daños a la infraestructura tecnológica, interceptación ilegítima de sistema informático o red de telecomunicación, suplantación de sitios web para capturar datos personales, acceso abusivo a un sistema informático y más delitos informáticos se aplicará la ley correspondiente derivando en las sanciones que este aplique.

Capítulo 4 Definición de roles y responsabilidades dentro de la organización.

4.1 Definición de rol y responsabilidad.

Se conoce a un rol como un conjunto de responsabilidades asignadas a un puesto de trabajo, es decir el comportamiento que se tiene frente a una actividad. Este rol se va a asociar con una persona física o a un equipo de personas estos pueden tener varios roles.

En cambio, una responsabilidad es aquella que es realizada por una o varias personas hasta completar una tarea.

Al definir los roles y responsabilidades dentro de una organización se deben contemplar las siguientes actividades (ISACA, 2018, p.58):

1. Establecer, acordar y comunicar los roles y responsabilidades relacionadas con TI a todo el personal, de acuerdo con las necesidades y objetivos. Delinear claramente las responsabilidades y la rendición de cuentas, especialmente para la toma de decisiones y aprobaciones.

2. Considerar los requisitos para la continuidad del negocio y del servicio de TI al definir los roles.

3. Proporcionar información al proceso de continuidad de servicios de TI, manteniendo la información de contacto y las descripciones de roles de la organización actualizados.

4. Incluir requisitos específicos en las descripciones de roles y responsabilidades relativos al cumplimiento de las políticas y procedimientos de gestión, el código ético y las prácticas profesionales.

5. Asegurar que se defina la rendición de cuentas a través de roles y responsabilidades.

6. Estructurar roles y responsabilidades para reducir la posibilidad de que un único rol comprometa un proceso crítico.

7. Implementar las prácticas de supervisión adecuadas para asegurar que los roles y responsabilidades se ejerzan adecuadamente, para asegurar que todo el personal tiene la autoridad y recursos suficientes para ejecutar sus roles y responsabilidades, y de forma general, para revisar el rendimiento. El nivel de supervisión debe alinearse con la sensibilidad del puesto y la extensión de las responsabilidades asignadas.

4.2 Delimitación de roles.

La delimitación de roles y responsabilidades se llevará a cabo por el Comité de Seguridad que tendrá como responsabilidad la revisión y actualización de políticas de Seguridad de la Información que se requiere para la implementación del SGSI.

Para mayor entendimiento se realizará una matriz en la cual se establecerán los roles y responsabilidades, así como la explicación detallada de lo que realiza cada rol dentro del área de informática del Municipio de Ecatepec de Morelos.

El Comité de Seguridad que estará a cargo de las Políticas de Seguridad que se implementarán dentro del municipio también estará encargado de evaluar los riesgos que se podrían presentar, dirigirá y controlará los procesos que estén enfocados a la seguridad dentro y fuera de la organización, definirá las estrategias que ayudaran a la organización a la toma de decisiones.

Algunas de las funciones que puede tener el Comité de Seguridad son las siguientes:

- El Comité de Seguridad de la Información será el primer nivel de aprobación, revisión, rechazo, modificación o eliminación de las políticas.
- Sugerir normas y procedimientos de Seguridad de la Información.
- Revisa, valida normas y procedimientos en general, todo con el fin de verificar que se estén cumpliendo los aspectos de seguridad.
- Por medio del Comité de Seguridad de la Información se supervisa y controla El Plan de Seguridad de la Información que es analizado, supervisado y controlado por el Comité de Seguridad de la Información para analizar temas tales como:
    - El avance del Plan de Seguridad y modificar el conjunto de normas en caso de atrasos.
    - Establecer recursos para administrar los incidentes de seguridad u otras vulnerabilidades.
- Es el encargado de hacer cumplir las políticas, normas, procedimientos y documentos relacionados con la Seguridad de la Información dentro de la organización.
- Monitorea cambios significativos en los riesgos que afectan a los recursos de la información del municipio frente a posibles amenazas, ya sean internas o externas.
- Toma en conocimiento y supervisa la investigación y monitoreo de los incidentes, relativos a la Seguridad de la Información, que se produzcan del municipio.
- Por medio del Comité de Seguridad de la Información se instruirá al encargado del área de informática el inicio del proceso de revisión de las políticas vigentes.
- Aprobar las principales iniciativas para incrementar la Seguridad de la Información de acuerdo con las competencias y responsabilidades asignadas, así como acordar y aprobar metodologías y procesos específicos relativos a la Seguridad de la Información.
- Evaluar y coordinar la implementación de controles específicos de Seguridad de la Información para los sistemas o servicios del municipio sean existentes o nuevos.

- Promover la difusión y apoyo a la Seguridad de la Información dentro del municipio.

El responsable del Comité de Seguridad de la Información es el encargado de coordinar que todos los puntos propuestos para el direccionamiento estratégico de los SGSI sean aplicados y respetados por toda la organización ya que requiere el compromiso, recursos y la asignación de las responsabilidades para llevar a cabo la administración de la Seguridad de la Información.

El comité está conformado de la siguiente manera:

- Coordinador del proyecto.
- Responsablede la Auditoría de Seguridad Informática (responsable del comité).
- Responsable del área de soporte.
- Responsable del área de redes.
- Responsable del área de secretaria.
- Responsable del área de Desarrollo web y Sistemas.

Los responsables estarán bajo la supervisión de cada encargado del área de informática.

4.3 Matriz de roles y responsabilidades de los integrantes del comité de Seguridad de la Información.

Tabla 2: roles y responsabilidades del Comité.

Área	Rol	Responsabilidad
Seguridad informática	Responsable del comité	Monitorear el cumplimiento de las políticas propuestas por el comité.
		Definir el ¿Cómo? Se implementarán los procedimientos del SGSI.
		Aprobar la documentación del SGSI.
		Coordinar todas las funciones relacionadas con el área de seguridad (física e información).
		Evaluar aspectos de seguridad respecto a implantaciones de las políticas establecidas por el comité.
		Verificar que cada activo de la información haya sido asignado a un propietario.
		Asegurar las responsabilidades de los empleados estén definidas.
		Definir un plan de comunicación entre empleados y los integrantes del comité.
		Realizar el seguimiento de los reportes de análisis de riesgos.
Área de soporte	Auditor	Analizar el proceso para la detección y eliminación de virus y/o amenazas detectadas.
		Evaluar el mantenimiento realizado al software utilizado.

Área	Rol	Responsabilidad
		Verificar si existe un procedimiento para la recuperación de datos.
		Verificar la existencia de un inventario de activos de información y si este se encuentra actualizado.
		Verificar si se cuenta con evidencia de accesos autorizados a la red interna.
		Proponer protocolos de seguridad contra el robo de información.
		Proponer software para la protección de información confidencial.
		Proponer políticas y esquemas de seguridad.
Área de redes	Auditor	Analizar los riesgos a los que se ve expuesto la red interna.
		Evaluar los recursos de red.
		Analizar el control de acceso y diseño de la red interna.
		Monitorear el mantenimiento y salvaguarda de instalaciones de red y equipo de conectividad.
		Evaluar la protección de la información de los diferentes sistemas operativos y bases de datos.
		Proponer protocolos y políticas para la correcta reacción para posibles incidentes de seguridad.
Área de secretaria	Auditor	Evaluar la infraestructura del área.
		Evaluar los recursos humanos.
		Evaluar el control de equipos (altas y bajas).
		Evaluar la comunicación hacia los empleados de las políticas de seguridad.
Área de desarrollo web y sistemas	Auditor	Evaluar la administración y configuración de los servicios web.
		Evaluar la administración de los sistemas de información.

Fuente: elaboración propia.

4.4 Matriz de roles y responsabilidades del personal del área de informática.

Tabla 3: roles y responsabilidades Área de Informática.

Área	Rol	Responsabilidad
Seguridad informática	Responsable del área	Monitorear el cumplimiento de las políticas propuestas por el comité.
		Evaluar el funcionamiento de las políticas implantadas por el comité seguridad.
		Definir el ¿Cómo? Se implementará los procedimientos del SGSI.
		Coordinar todas las funciones relacionadas con el área de seguridad (física y lógica).

Área	Rol	Responsabilidad
		Verificar que cada activo de la información haya sido asignado a un propietario.
		Delimitar los roles y las responsabilidades.
		Implementar una correcta comunicación entre el personal y los integrantes del comité de seguridad.
Área de soporte	Soporte técnico	Detección y eliminación de amenazas.
		Realización de mantenimiento preventivo y correctivo de los activos.
		En conjunto con el responsable del área realizar la asignación de activos de información a un propietario.
		Activación de licencias de software (paquetería, antivirus, etc.)
		Evaluar la protección de la información de los diferentes sistemas operativos y bases de datos
Área de redes	Responsable de redes	Evaluar la infraestructura de red.
		Evaluación del acceso a internet.
		Monitorear el mantenimiento y salvaguarda de instalaciones de red y equipo de conectividad.
		Mantener firewalls y filtros de seguridad actualizados.
		Mantener comunicación con los proveedores de la red.
		Evaluar la protección de la información de los diferentes sistemas operativos y bases de datos
Área de secretaria	Secretaría	Mantener actualizada la estructura organizacional.
		Control de equipos (altas y bajas).
		Comunicación de las políticas de seguridad.
		Promover las políticas de seguridad.
Área de desarrollo web y sistemas	Responsable del desarrollo web y sistemas	Evaluar la administración y configurar de todo el servicio Web

Fuente: elaboración propia.

4.5 Identificación de activos.

El área de informática no contaba con un inventario así que se creó un inventario adecuado con una clave, la cual sirve como identificador para cada uno de los activos existentes en el área. Las claves con las que se identificarán los activos están conformadas por letras que se asemejan al nombre del activo y números, quedando las siguientes:

- SERV01: servidores.
- COM01A: computadoras.

- IMP01A: impresoras.
- SIL01AS: sillas.
- AN01EL: anaqueles.
- TEL 001: teléfonos.
- RACK001: rack.

Tabla 4: activos.

Identificación de activos	**Activo**	**Características**	**Localización**	**Estado**
SERV01	Servidor	Información no proporcionada	Soporte Técnico y Redes	Bueno
SERV02				
SERV03				
COM04A	Computadora	WIN 7, 64 BITS, 4GB RAM, 500GB HDD, con HDD EXTRAIBLE DE 1TB		
COM05A		WIN 7 PROFESIONAL, 64 BITS, 4GB RAM, 1TB HDD		
COM06A	Computadora	WIN 10 32 BITS, 2GB RAM, 120GB HDD		
IMP04A	Impresora	HP	Soporte Técnico y Redes	Bueno
SIL09AS	Silla	Silla negra con ruedas		
SIL10AS				
SIL11AS				

Identificación de activos	Activo	Características	Localización	Estado
SIL12AS				
SIL13AS				
RACK001	Rack	Información no proporcionada		
COM01A	Computadora	WIN 7, COMPAQ PRESARIO, INTEL CELERON, 2GB RAM, 250GB ROM HDD		Bueno
COM02A		WIN 10, 4GB RAM, 64 BITS, 500GB HDD		Regular
IMP01A	Impresora	HP		
IMP02A	Multifuncional	HP		
SIL01AS				
SIL02AS				
SIL03AS	Silla	Silla negra de ruedas		Bueno
SIL04AS				
AN01EL	Anaquel	Anaquel de tres secciones de metal		
AN02EL				

Identificación de activos	**Activo**	**Características**	**Localización**	**Estado**
TEL001	Teléfono	Teléfono alámbrico de la compañía de teléfonos		
TEL002				
COM03A	Computadora	WIN 8, 32BITS, 2GB RAM, 1TB HDD	Almacén	Bueno
IMP03A	Impresora	Multifuncional Samsung		Excelente
SIL05AS	Silla	Silla negra de ruedas		Bueno
SIL06AS				
SIL07AS				
SIL08AS				

Fuente: elaboración propia.

Capítulo 5 Aplicación de la metodología OCTAVE

5.1 ¿Qué es OCTAVE?

OCTAVE se centra en los activos de información en el contexto de cómo se usa, donde se almacenan, transportan y procesan, y como están expuestos a amenazas, vulnerabilidades e interrupciones.

Caralli, R. (2007) define como aquella metodología que identifica y evalúa los riesgos de Seguridad de la Información. Esta ayuda a desarrollar criterios de evaluación para riesgos cualitativos, identificar los activos que son importantes para la organización, identificación de vulnerabilidades y amenazas y determinar y evaluar las posibles consecuencias en caso de existir vulnerabilidades.

5.2 Metodología.

Caralli, R. (2007) refiere que este método consta de ocho pasos que se organizan en tres fases:

Tabla 5: fases de Metodología OCTAVE.

Fase	Descripción	Paso
Fase 1	El equipo de análisis identifica los activos importantes relacionados con la información y la estrategia de protección actual para esos activos, luego determina cuales de los activos son críticos para la organización.	Paso 1 Establecer criterios de medición de riesgos. Paso 2 Desarrollo de un perfil de activos de información. Paso 3 Identificación de los contenedores de activos de información.
Fase 2	El equipo de análisis realiza una evaluación de la infraestructura de información para complementar el análisis de amenazas realizado en la fase 1.	Paso 4 Identificación de áreas de preocupación Paso 5 Identificación de escenarios de amenaza.
Fase 3	El equipo de análisis realiza actividades de identificación de riesgos y desarrolla un plan de mitigación para los activos críticos.	Paso 6 Identificación de riesgos. Paso 7 Analizar riesgos. Paso 8 Mitigación de riesgos.

Fuente: Caralli, R. (2007). Cap.3 Introducing OCTAVE Allegro (pp.17-21).

Estos pasos se desglosan de la siguiente manera:

Paso 1: establecer criterios de medición de riesgos.

Los criterios de medición de riesgos son un conjunto de medidas cualitativas contra las cuales los efectos de un riesgo realizado pueden evaluarse y formar la base para la evaluación de riesgo de activos de información.

Paso 2: desarrollo de un perfil de activos de información.

En este paso, se comienza con el proceso de definir los activos de información, se crea un perfil para cada activo de información que es la base para la identificación de amenazas y riesgos en pasos posteriores.

Un perfil es una representación de un activo de información que describe sus características, cualidades y valor. El proceso de creación de perfiles garantiza que un activo se describa de manera clara y coherente.

Paso 3: identificación de los contenedores de activos de información.

En este paso es necesario que se identifique todos los contenedores en los que se almacena un activo, definiendo así los límites y circunstancias en las que deben ser examinadas por riesgo.

Estos contenedores generalmente se identifican como algún tipo de activo técnico: hardware, software o un sistema, pero un contenedor también puede ser un objeto físico como una hoja de papel o una persona que es importante para la organización.

Paso 4: identificación de áreas de preocupación.

Comienza el proceso de identificación de riesgos mediante las posibles condiciones o situaciones que pueden amenazar el activo de información, mediante la lluvia de ideas acerca de posibles condiciones o situaciones que puedan amenazar el activo de la información.

Paso 5: identificación de escenarios de amenaza.

En este paso se expanden los escenarios de amenazas que previamente se presentaron en el paso anterior, mediante un árbol de amenazas.

Tabla 6: árbol de amenazas.

Árbol de amenazas	Definición
Actores humanos utilizando medios técnicos.	Las amenazas en esta categoría representan amenazas al activo de información a través de infraestructura técnica de la organización o por acceso directo a un contenedor (tecnología activo físico) que aloja un activo de

Árbol de amenazas	Definición
	información. Requieren la acción directa de una persona y puede ser de naturaleza deliberada o accidental.
Actores humanos utilizando a medios físicos.	Las amenazas en esta categoría representan amenazas al activo de información que son el resultado del acceso físico al activo o un contenedor que alberga una información. Requieren la acción directa de una persona y pueden ser deliberados o accidentales.
Problemas técnicos.	Las amenazas en esta categoría son problemas con la información de una organización. Los ejemplos incluyen defectos de hardware, defectos de software, datos, códigos maliciosos (p. ej., virus) y otros problemas relacionados con el sistema.
Otros problemas.	Las amenazas en esta categoría son problemas o situaciones que están fuera de control de una organización. Esta categoría de amenazas incluye desastres naturales (por ejemplo, inundaciones, terremotos) y riesgos de interdependencia. Incluye la falta de disponibilidad de infraestructuras críticas (p. ej., suministro de energía).

Fuente: Caralli, R. (2007). Cap.3 Introducing OCTAVE Allegro (p. 19).

Paso 6: identificación de riesgos.

En el paso anterior se identificaron las amenazas, y en este paso se plantea las consecuencias para una organización. Una amenaza puede tener múltiples impactos potenciales en una organización.

Paso 7: analizar riesgos.

Es una medida cuantitativa, en donde se establece la medida en que la organización se ve afectada por las amenazas.

Aquí se define la consecuencia de que un riesgo impacta a la organización contra la importancia en diversas áreas de impacto, por ejemplo, si la reputación es lo más importante para una organización entonces los riesgos que tengan mayor impacto en la reputación generan puntajes con impactos y probabilidad más alta.

Paso 8: mitigación de riesgos

En esta etapa se realiza una estrategia de mitigación de riesgos, se realiza con base a los puntajes de riesgo, mismos que son priorizados.

5.3 Aplicación de OCTAVE dentro del área.

5.3.1 Fase 1: criterios de medición de riesgos.

En esta fase se establecerán los criterios de medición, los cuales permitirán medir el efecto de los riesgos sobre la organización, considerando las siguientes áreas de impacto:

- Reputación – Confianza del cliente
- Financiero
- Productividad
- Seguridad y Salud
- Multas – Sanciones Legales

5.3.1.1 Reputación – Confianza del Cliente.

Esta área de impacto está relacionada con la imagen del municipio, ya que esta se puede ver afectada a raíz de un incidente de seguridad ya que este maneja información sensible de los contribuyentes, empleados, proveedores etc.

Tabla 7: criterio de medición de riesgos.

Hoja de Trabajo 1	**Criterio de Medición de Riesgo** Reputación – Confianza del cliente		
Área de Impacto	**Alto**	**Medio**	**Bajo**
Afectación a la imagen de la organización	La información relacionada con el incidente de seguridad se conoce públicamente.	La información relacionada con el incidente de seguridad se conoce dentro de la organización.	La información relacionada con incidente de seguridad se conoce dentro del área de informática.

Fuente: elaboración propia.

5.3.1.2 Financiero.

Corresponde al área operativa donde el control principal es evitar pérdidas por fallo en los sistemas, errores humanos o acontecimientos externos. Este impacto influye a los impactos de Reputación y Multas – Sanciones Legales.

Tabla 8: criterio de medición de riesgo financiero.

Hoja de Trabajo 2	**Criterio de Medición de Riesgo Financiero**		
Área de Impacto	**Alto**	**Medio**	**Bajo**
Riesgo Operativo	Perdida potencial de los sistemas de información y controles internos de seguridad.	Perdida potencial de los sistemas de información y controles internos de seguridad derivados de errores humanos.	Perdida potencial de los sistemas de información y controles internos de seguridad derivados de fallas administrativas.

Fuente: elaboración propia.

5.3.1.3 Productividad.

Se establece por ley que el personal que labora dentro del área informática su jornada será de 8 horas diarias de lunes a viernes, sin embargo, hay personal que decide extender su jornada, entre mayor tiempo y genera más agotamiento, esto trae repercusiones con productividad dentro de la organización.

Tabla 9: criterio de medición de riesgos de productividad.

Hoja de Trabajo 3	**Criterio de Medición de Riesgo Productividad**		
Área de Impacto	**Alto**	**Medio**	**Bajo**
Horas de trabajo del personal	Las horas de trabajo del personal se incrementaron en mas 3 horas por día.	Las horas de trabajo del personal se incrementaron entre 1 y 3 horas por día.	Las horas de trabajo del personal se incrementan en menos de 1 hora por día.

Fuente: elaboración propia.

5.3.1.4 Seguridad y Salud.

Este criterio se enfoca en la salud y seguridad del personal.

Tabla 10: criterio de medición de riesgos de seguridad y salud.

Hoja de Trabajo 4	**Criterio de Medición de Riesgo Seguridad y Salud**		
Área de Impacto	**Alto**	**Medio**	**Bajo**
Vida	Existe perdida de la vida del personal	La vida del personal está amenazada	No hay perdida o amenaza significativa de los empleados
Salud	Deterioro permanente de la salud del personal	Impedimento de realizar las actividades en su lugar de trabajo	Mínima afectación de los empleados

Fuente: elaboración propia.

5.3.1.5 Multas – Sanciones Legales.

Tabla 11: criterio de medición de riesgos multas y sanciones legales.

Hoja de Trabajo 5	**Criterio de Medición de Riesgo Multas – Sanciones Legales**		
Área de Impacto	**Alto**	**Medio**	**Bajo**
Investigaciones	Gobierno estatal / federal u otra organización inicia una investigación de profundidad sobre el tratamiento de la información.	Gobierno estatal / federal u otra organización solicita información o registros.	No hay investigaciones de gobierno estatal / federal u otra organización.
Multas	Multas mayores a $250,000	Multas entre $100,000 y $250,000	Multas menores a $100,000

Fuente: elaboración propia.

5.3.1.6 Priorización de las Áreas de Impacto.

De acuerdo con las hojas de trabajo anteriores se generó la siguiente tabla, donde establece el área con mayor importancia otorgándole una puntuación de 5 que es el valor más alto.

Tabla 12: priorización de las áreas de impacto.

Hoja de Trabajo 6	**Priorización de las Áreas de Impacto**
Prioridad	**Áreas de Impacto**
5	Financiero

Hoja de Trabajo 6	Priorización de las Áreas de Impacto
Prioridad	**Áreas de Impacto**
4	Multas – Sanciones Legales
3	Reputación – Confianza del cliente
2	Seguridad y Salud
1	Productividad

Fuente: elaboración propia.

5.3.2 Fase 1: perfil de activos de información.

Tabla 13: perfil de activos de información.

Hoja de trabajo 7	Perfil de activo de información	
Activo Crítico:	Correo Electrónico	
Descripción:	Es un servicio de red que permite a los usuarios el intercambio de información mediante una infraestructura de red.	
Fecha de creación:	11/03/20	
Titular del activo:	Área de redes / Proveedor	
Contenedor para los activos de la información		
Hardware:	Servidor	
Requerimientos de Seguridad		
Confidencialidad:	Todos los correos electrónicos recibidos por el área de informática se consideran como información confidencial.	
Integridad:	La información enviada o recibida por personal del área debe ser correcta.	
Disponibilidad:	La información recabada por este medio debe de estar disponible para cuando esta sea necesaria.	
Valoración		
Confidencialidad:	**Integridad:**	**Disponibilidad:** ×
Perfil de activo de información		
Activo Crítico:	Base de Datos	

Hoja de trabajo 7	Perfil de activo de información	
Descripción:	Es una herramienta que se utiliza para almacenar, recopilar y organizar información.	
Fecha de creación:	11/03/20	
Titular del activo:	Área de soporte	
Contenedor para los activos de la información		
Hardware:	Servidor físico	
Requerimientos de Seguridad		
Confidencialidad:	Los datos registrados solo están disponibles para aquellos empleados que tengan autorización.	
Integridad:	Los datos no han sufrido una transformación o modificación desde su generación sin previa autorización.	
Disponibilidad:	Los datos almacenados estarán disponibles para los usuarios autorizados.	
Valoración		
Confidencialidad: ×	**Integridad:**	**Disponibilidad:** ×
Perfil de activo de información		
Activo Crítico:	Servidores	
Descripción:	Es un equipo que forma parte de una red informática y provee servicios a otros equipos.	
Fecha de creación:	11/03/20	
Titular del activo:	Área de redes	
Contenedor para los activos de la información		
Hardware:	Servidor físico	
Requerimientos de Seguridad		
Confidencialidad:	La configuración de los servidores será hecha únicamente por el encargado.	
Integridad:	Las actualizaciones de seguridad y los estándares de configuración deberán ser aplicados correctamente y en un periodo de tiempo establecido.	

Hoja de trabajo 7	Perfil de activo de información	
	Los servidores deben de estar protegidos físicamente (control de acceso y protección ambiental).	
Disponibilidad:	El uso de copias de seguridad periódicas divididas en bloques garantizaran la disponibilidad de estos.	
Valoración		
Confidencialidad:	**Integridad: ×**	**Disponibilidad:**
Perfil de activo de información		
Activo Crítico:	Computadoras (PC)	
Descripción:	Es una maquina capaz de recibir, almacenar y procesar información mediante software.	
Fecha de creación:	11/03/20	
Titular del activo:	Área de soporte / Área de secretaria	
Contenedor para los activos de la información		
Hardware:	Computadoras (PC)	
Requerimientos de Seguridad		
Confidencialidad:	Para el acceso a los equipos de cómputo (PC) será mediante claves, en el tiempo de inactividad estos serán bloqueados por los usuarios.	
Integridad:	Se mantendrá actualizado el sistema operativo, antivirus, etc. El acceso a estos solo estará en áreas con personal autorizado.	
Disponibilidad:	El equipo de cómputo estará disponible para aquellos usuarios autorizados.	
Valoración		
Confidencialidad:	**Integridad: ×**	**Disponibilidad:**
Perfil de activo de información		
Activo Crítico:	Servicios de Red	
Descripción:	Conjunto de nodos (computadoras) conectados entre sí con la finalidad de compartir información, recursos, etc.	
Fecha de creación:	11/03/20	

Hoja de trabajo 7	Perfil de activo de información	
Titular del activo:	Área de redes	
Contenedor para los activos de la información		
Hardware:	N/A	
Requerimientos de Seguridad		
Confidencialidad:	Se limitará el uso de operaciones remotas y se hará uso de autorización para los usuarios.	
Integridad:	Uso de autentificación de usuarios para el acceso a datos dentro de la red.	
Disponibilidad:	Los equipos conectados podrán acceder a datos y recursos de la red.	
Valoración		
Confidencialidad:	**Integridad:**	**Disponibilidad: ×**
Perfil de activo de información		
Activo Crítico:	Mensajería instantánea	
Descripción:	Es una comunicación en tiempo real entre dos o más personas.	
Fecha de creación:	11/03/20	
Titular del activo:	Proveedor	
Contenedor para los activos de la información		
Hardware:	Dispositivos móviles	
Requerimientos de Seguridad		
Confidencialidad:	Se debe de evitar él envió de documentos o información sensible a través de estas aplicaciones.	
Integridad:	Cada dispositivo móvil en el que se encuentre una o más aplicaciones de mensajería instantánea debe contar con un programa antivirus el cual busca la protección a cualquier programa malicioso.	
Disponibilidad:	La comunicación empleada es realizada en tiempo real.	
Valoración		

Hoja de trabajo 7	Perfil de activo de información	
Confidencialidad: ×	**Integridad:**	**Disponibilidad:**
Perfil de activo de información		
Activo Crítico:	Empleados	
Descripción:	Es aquella persona física capaz de brindar servicios	
Fecha de creación:	11/03/20	
Titular del activo:	Área de Recursos Humanos	
Contenedor para los activos de la información		
Hardware:	N/A	
Requerimientos de Seguridad		
Confidencialidad:	El personal deberá contar con un acuerdo de confidencialidad en donde se indique que el uso de la información se limitará para fines laborales.	
Integridad:	N/A	
Disponibilidad:	El personal estará disponible dentro del horario laboral.	
Valoración		
Confidencialidad:	**Integridad:**	**Disponibilidad:** ×

Fuente: elaboración propia.

5.3.3 Fase 1: identificación de los contenedores de activos de información.

Tabla 14: contenedores de activos de información.

Hoja de trabajo 8	Contenedor interno
Nombre	**Propietario**
Plataforma de correo	Área de redes / Proveedor
USB	Empleados
Disco duro	Área de Soporte / Empleados
Archivos físicos	Área secretaria / Empleados
Base de datos	Área de soporte

Fuente: elaboración propia.

5.3.4 Fase 2: identificación de áreas de preocupación.

Tabla 15: áreas de preocupación.

Hoja de trabajo 9	Áreas de Preocupación
Acceso no autorizado a los sistemas informáticos.	
Bloqueo de los equipos por inactividad nulo.	
Medios de almacenamiento físicos expuestos a personas externas.	
Problemas de conectividad en la red interna.	
Problemas de conectividad con el servicio de internet.	
Fallo, desactualización o defecto del software.	
Fallo del hardware.	
Bloqueo a los accesos al edificio.	
Interrupción del servicio eléctrico.	
Crisis de seguridad.	
Políticas no establecidas u obsoletas.	
Sanciones no establecidas.	
No existe una evaluación e identificación de riesgos y amenazas.	
No existe un tratamiento contra las amenazas encontradas.	
Los controles físicos de acceso no están actualizados (Acceso de personas ajenas del área al equipo de cómputo).	
Mala aplicación de controles lógicos.	
Acceso a redes sociales.	

Fuente: elaboración propia.

5.3.5 Fase 2: identificación de escenarios de amenaza.

Tabla 16: escenarios de amenazas.

Hoja de trabajo 10	Escenarios	
Árbol de amenaza	**Área de preocupación**	**Resultado**
Actores humanos utilizando medios técnicos	Exposición de los activos de la información, acceso no autorizado a los sistemas informáticos.	Divulgación
	Exposición de los activos de la información, bloqueo de los equipos por inactividad.	Modificación / Divulgación
	Exposición de los activos de la información, mala aplicación de controles lógicos.	Modificación / Divulgación
	Exposición de los activos de la información, acceso a redes sociales.	Divulgación
Actores humanos utilizando medios físicos	Exposición de los activos de la información, medios de almacenamiento físicos expuestos a personas externas.	Modificación / Divulgación
	Exposición de los activos de la información, los controles físicos de acceso no están actualizados (Acceso de personas ajenas del área al equipo de cómputo).	Modificación / Divulgación
Problemas técnicos	Problemas de conectividad en la red interna.	Interrupción

Hoja de trabajo 10	Escenarios	
Árbol de amenaza	**Área de preocupación**	**Resultado**
	Problemas de conectividad con el servicio de internet.	Interrupción
	Fallo, desactualización o defecto del software.	Interrupción
	Fallo del hardware.	Interrupción
Otros problemas	Bloqueo a los accesos al edificio.	Interrupción
	Interrupción del servicio eléctrico.	Interrupción
	Crisis de seguridad.	Interrupción
	Políticas no establecidas u obsoletas.	Interrupción
	Sanciones no establecidas	Interrupción
	No existe una evaluación e identificación de riesgos y amenazas.	Interrupción
	No existe un tratamiento contra las amenazas encontradas.	Interrupción

Fuente: elaboración propia.

5.3.6 Fase 3: identificación de riesgos.

Tabla 17: riesgos.

Hoja de trabajo 11	Consecuencias de los activos de la información
Acceso no autorizado a los sistemas informáticos.	
Bloqueo de los equipos por inactividad.	
Mala aplicación de controles lógicos.	
Acceso a redes sociales.	
Medios de almacenamiento físicos expuestos a personas externas.	
Los controles físicos de acceso no están actualizados (Acceso de personas ajenas del área al equipo de cómputo).	
Problemas de conectividad en la red interna.	
Problemas de conectividad con el servicio de internet.	
Fallo, desactualización o defecto del software.	
Fallo del hardware.	
Bloqueo a los accesos al edificio.	
Interrupción del servicio eléctrico.	
Crisis de seguridad.	
Políticas no establecidas u obsoletas.	
Sanciones no establecidas.	
No existe una evaluación e identificación de riesgos y amenazas.	
No existe un tratamiento contra las amenazas encontradas.	

Fuente: elaboración propia.

5.3.7 Fase 3: analizar riesgos.

Tabla 18: análisis de riesgos.

Hoja de trabajo 12	**Análisis de riesgos**			
Área de preocupación	Área de impacto	Ranking	Impacto	Score
Acceso no autorizado a los sistemas informáticos	Financiero	5	Alto (3)	15
	Multas – Sanciones Legales	4	Alto (3)	12
	Reputación – Confianza del cliente	3	Alto (3)	9
	Seguridad y Salud	2	Bajo (1)	2
	Productividad	1	Alto (3)	3
				Total: 41
Bloqueo de los equipos por inactividad	Financiero	5	Medio (2)	10
	Multas – Sanciones Legales	4	Bajo (1)	4
	Reputación – Confianza del cliente	3	Medio (2)	6
	Seguridad y Salud	2	Bajo (1)	2
	Productividad	1	Bajo (1)	1
				Total:23
Mala aplicación de controles lógicos	Financiero	5	Alto (3)	10
	Multas – Sanciones Legales	4	Alto (3)	12
	Reputación – Confianza del cliente	3	Medio (2)	6
	Seguridad y Salud	2	Bajo (1)	2
	Productividad	1	Bajo (1)	1
				Total:31
Acceso a redes sociales	Financiero	5	Bajo (1)	5
	Multas – Sanciones Legales	4	Medio (2)	8
	Reputación – Confianza del cliente	3	Alto (3)	9
	Seguridad y Salud	2	Bajo (1)	2
	Productividad	1	Bajo (1)	1
				Total: 25
Medios de almacenamiento físicos expuestos a personas externas	Financiero	5	Medio (2)	10
	Multas – Sanciones Legales	4	Medio (2)	8
	Reputación – Confianza del cliente	3	Medio (2)	6
	Seguridad y Salud	2	Bajo (1)	2
	Productividad	1	Bajo (1)	1
				Total: 27
Los controles físicos de acceso no están actualizados (Acceso de personas ajenas	Financiero	5	Alto (3)	15
	Multas – Sanciones Legales	4	Alto (3)	12
	Reputación – Confianza del cliente	3	Alto (3)	9
	Seguridad y Salud	2	Medio (2)	4

Hoja de trabajo 12	**Análisis de riesgos**			
Área de preocupación	Área de impacto	Ranking	Impacto	Score
del área al equipo de cómputo)	Productividad	1	Alto (3)	3
				Total: 43
Problemas de conectividad en la red interna	Financiero	5	Bajo (1)	5
	Multas – Sanciones Legales	4	Bajo (1)	4
	Reputación – Confianza del cliente	3	Medio (2)	6
	Seguridad y Salud	2	Bajo (1)	2
	Productividad	1	Bajo (1)	1
				Total:18
Problemas de conectividad con el servicio de internet	Financiero	5	Medio (2)	10
	Multas – Sanciones Legales	4	Bajo (1)	4
	Reputación – Confianza del cliente	3	Bajo (1)	9
	Seguridad y Salud	2	Bajo (1)	2
	Productividad	1	Alto (3)	3
				Total: 28
Fallo, desactualización o defecto del software	Financiero	5	Alto (3)	15
	Multas – Sanciones Legales	4	Medio (2)	8
	Reputación – Confianza del cliente	3	Bajo (1)	3
	Seguridad y Salud	2	Bajo (1)	2
	Productividad	1	Bajo (1)	1
				Total:29
Fallo del hardware	Financiero	5	Alto (2)	10
	Multas – Sanciones Legales	4	Bajo (1)	4
	Reputación – Confianza del cliente	3	Medio (2)	6
	Seguridad y Salud	2	Bajo (1)	2
	Productividad	1	Alto (3)	3
				Total:25
Bloqueo a los accesos del edificio	Financiero	5	Alto (3)	15
	Multas – Sanciones Legales	4	Medio (2)	8
	Reputación – Confianza del cliente	3	Alto (3)	9
	Seguridad y Salud	2	Medio (2)	4
	Productividad	1	Alto (3)	3
				Total:39
Interrupción del servicio eléctrico	Financiero	5	Bajo (1)	5
	Multas – Sanciones Legales	4	Bajo (1)	4
	Reputación – Confianza del cliente	3	Bajo (1)	3
	Seguridad y Salud	2	Bajo (1)	2
	Productividad	1	Alto (3)	3

Hoja de trabajo 12	**Análisis de riesgos**			
Área de preocupación	Área de impacto	Ranking	Impacto	Score
				Total:17
Crisis de seguridad	Financiero	5	Bajo (1)	5
	Multas – Sanciones Legales	4	Medio (2)	8
	Reputación – Confianza del cliente	3	Bajo (1)	3
	Seguridad y Salud	2	Medio (2)	4
	Productividad	1	Alto (3)	3
				Total:23
Políticas no establecidas u obsoletas	Financiero	5	Medio (2)	10
	Multas – Sanciones Legales	4	Bajo (1)	4
	Reputación – Confianza del cliente	3	Medio (2)	6
	Seguridad y Salud	2	Bajo (1)	2
	Productividad	1	Bajo (1)	1
				Total:23
Sanciones no establecidas	Financiero	5	Medio (2)	10
	Multas – Sanciones Legales	4	Bajo (1)	4
	Reputación – Confianza del cliente	3	Medio (2)	6
	Seguridad y Salud	2	Bajo (1)	2
	Productividad	1	Medio (2)	2
				Total:24
No existe una evaluación e identificación de riesgos y amenazas	Financiero	5	Alto (3)	15
	Multas – Sanciones Legales	4	Alto (3)	12
	Reputación – Confianza del cliente	3	Medio (2)	6
	Seguridad y Salud	2	Alto (3)	6
	Productividad	1	Medio (2)	2
				Total:41
No existe un tratamiento contra las amenazas encontradas	Financiero	5	Medio (2)	10
	Multas – Sanciones Legales	4	Bajo (1)	4
	Reputación – Confianza del cliente	3	Medio (2)	6
	Seguridad y Salud	2	Medio (2)	4
	Productividad	1	Bajo (1)	1
				Total:25

Fuente: elaboración propia.

5.3.8 Fase 3: mitigación de riesgos.

Tabla 19: mitigación de riesgos.

Matriz de Riesgos Relativos			
Probabilidad	Puntaje de Riesgo		
	30 a 45	16 a 29	0 a 15
Alta	Grupo 1 45	Grupo 2 29	Grupo 2 15
Media	Grupo 2 40	Grupo 2 25	Grupo 3 10
Baja	Grupo 3 30/35	Grupo 3 15/20	Grupo 4 5

Fuente: elaboración propia.

Tabla 20: enfoque de mitigación.

Grupo	Enfoque de Mitigación
Grupo 1	Mitigar
Grupo 2	Mitigar o Transferir
Grupo 3	Transferir o Aceptar
Grupo 4	Aceptar

Fuente: elaboración propia.

Tabla 21: mitigación de riesgos.

Hoja de trabajo 13	**Mitigación de riesgos**		
Área de preocupación: Acceso no autorizado a los sistemas informáticos.			
Puntaje de riesgo relativo	**Probabilidad subjetiva**	**Categoría**	**Acción**
41	Alta	Grupo 1	Mitigar
Control: El área de soporte proporcionara las claves autorizadas para los nuevos usuarios. El área de soporte mantendrá un registro de los usuarios y las claves de estos. El usuario que olvide o requiera cambiar sus claves deberá solicitar al área de soporte la reposición de estas. El área de soporte y los encargados de cada área delimitaran los accesos de información a los usuarios.			
Área de preocupación: Bloqueo de los equipos por inactividad.			
Puntaje de riesgo relativo	**Probabilidad subjetiva**	**Categoría**	**Acción**
23	Baja	Grupo 3	Transferir o Aceptar
Control: El encargado del área de secretaria y soporte implementará políticas de escritorio limpio y desatendido. Los usuarios de cada equipo de cómputo utilizaran el bloqueo por inactividad cuando estos se alejen de su equipo.			

Hoja de trabajo 13	**Mitigación de riesgos**		
Área de preocupación: Mala aplicación de controles lógicos.			
Puntaje de riesgo relativo	**Probabilidad subjetiva**	**Categoría**	**Acción**
31	Baja	Grupo 3	Transferir o Aceptar
Control: El área de soporte proporcionara las claves autorizadas para los nuevos usuarios. El área de soporte mantendrá un registro de los usuarios y las claves de estos. El usuario que olvide o requiera cambiar sus claves deberá solicitar al área de soporte la reposición de estas. El área de soporte y los encargados de cada área delimitaran los accesos de información a los usuarios.			
Área de preocupación: Acceso a redes sociales.			
Puntaje de riesgo relativo	**Probabilidad subjetiva**	**Categoría**	**Acción**
25	Medio	Grupo 2	Mitigar o Aceptar
Control: El encargado de sistemas será el responsable de bloquear las URL de redes sociales.			
Área de preocupación: Medios de almacenamiento físicos expuestos a personas externas.			
Puntaje de riesgo relativo	**Probabilidad subjetiva**	**Categoría**	**Acción**
27	Medio	Grupo 2	Mitigar o Aceptar
Control: Los usuarios resguardaran en su escritorio o cajón designado los medios de almacenamiento. El área de soporte proporcionara los medios de almacenamiento físicos.			
Área de preocupación: Los controles físicos de acceso no están actualizados (Acceso de personas ajenas del área al equipo de cómputo).			
Puntaje de riesgo relativo	**Probabilidad subjetiva**	**Categoría**	**Acción**
43	Alta	Grupo 1	Mitigar
Control: El encargado de seguridad informática implementara y delimitara el acceso al área de informática por parte de externos y/o proveedores. El encargado del área de secretaria notificara la llegada.			
Área de preocupación: Problemas de conectividad en la red interna.			
Puntaje de riesgo relativo	**Probabilidad subjetiva**	**Categoría**	**Acción**
18	Bajo	Grupo 3	Transferir o Aceptar
Control:			

Hoja de trabajo 13	Mitigación de riesgos		
Los encargados de las áreas de soporte y de redes serán los encargados de mantener el acceso a la red interna del municipio y notificar si esta está fallando a todas las áreas.			
Área de preocupación: Problemas de conectividad con el servicio de internet.			
Puntaje de riesgo relativo	**Probabilidad subjetiva**	**Categoría**	**Acción**
28	Medio	Grupo 2	Mitigar o Transferir
Control: Los encargados de las áreas de soporte y de redes serán los encargados de mantener el acceso a la red, estos notificaran a las áreas que si el servicio es interrumpido. Los encargados de las áreas de soporte y de redes se pondrán en contacto con el proveedor para reportar el fallo del servicio. Los encargados de las áreas de soporte y de redes darán seguimiento hasta que el servicio sea restablecido.			
Área de preocupación: Fallo, desactualización o defecto del software.			
Puntaje de riesgo relativo	**Probabilidad subjetiva**	**Categoría**	**Acción**
29	Medio	Grupo 2	Mitigar o Transferir
Control: El encargado del área de soporte mantendrá un plan de mantenimiento para los equipos de cómputo.			
Área de preocupación: Fallo del hardware.			
Puntaje de riesgo relativo	**Probabilidad subjetiva**	**Categoría**	**Acción**
25	Medio	Grupo 2	Mitigar o Transferir
Control: El encargado del área de soporte mantendrá un plan de mantenimiento para los equipos de cómputo. El usuario notificara a el área de soporte el fallo del hardware de su equipo.			
Área de preocupación: Bloqueo a los accesos del edificio.			
Puntaje de riesgo relativo	**Probabilidad subjetiva**	**Categoría**	**Acción**
39	Medio	Grupo 2	Mitigar o Transferir
Control: Los encargados de las áreas definirán un plan de contingencias para buscar la protección de vidas humanas y activos de información.			
Área de preocupación: Interrupción del servicio eléctrico.			
Puntaje de riesgo relativo	**Probabilidad subjetiva**	**Categoría**	**Acción**
17	Bajo	Grupo 3	Transferir o Aceptar

Hoja de trabajo 13	**Mitigación de riesgos**		
Control: Los encargados de las áreas de soporte y de redes darán seguimiento hasta que el servicio sea restablecido y notificarán sobre la interrupción del servicio.			
Área de preocupación: Crisis de seguridad.			
Puntaje de riesgo relativo	**Probabilidad subjetiva**	**Categoría**	**Acción**
23	Medio	Grupo 2	Mitigar o Transferir
Control: Los encargados de las áreas definirán un plan de contingencias para buscar la protección de vidas humanas y activos de información.			
Área de preocupación: Políticas no establecidas u obsoletas.			
Puntaje de riesgo relativo	**Probabilidad subjetiva**	**Categoría**	**Acción**
23	Medio	Grupo 2	Mitigar o Transferir
Control: Los encargados de seguridad informática y secretaria establecerán nuevas políticas y estos serán los encargados de comunicárselo a todas las áreas**.**			
Área de preocupación: Sanciones no establecidas.			
Puntaje de riesgo relativo	**Probabilidad subjetiva**	**Categoría**	**Acción**
24	Medio	Grupo 2	Mitigar o Transferir
Control: Los encargados de las áreas de seguridad informática y secretaria diseñaran, aplicaran y ejecutaran las sanciones correspondientes al no cumplirse las políticas.			
Área de preocupación: No existe una evaluación e identificación de riesgos y amenazas.			
Puntaje de riesgo relativo	**Probabilidad subjetiva**	**Categoría**	**Acción**
41	Alta	Grupo 1	Mitigar
Control: El encargado de seguridad informática implementara una evaluación e identificación de riesgos ya sea de manera autónoma o con ayuda de un proveedor en materia de TI.			
Área de preocupación: No existe un tratamiento contra las amenazas encontradas.			
Puntaje de riesgo relativo	**Probabilidad subjetiva**	**Categoría**	**Acción**
25	Medio	Grupo 2	Mitigar o Transferir
Control: El encargado de seguridad informática buscara un tratamiento contra las amenazas y darles el seguimiento debido.			

Fuente: elaboración propia.

Capítulo 6 Propuesta de selección e implementación de controles de seguridad.

6.1 Controles de Seguridad.
Al definir un control se dice que es aquella medida que se utiliza para mitigar el riesgo dentro de una organización.

Dicho esto, para la selección de los controles de seguridad se realiza con base a la gestión de riesgos, es decir, el riesgo para las operaciones y los activos de la organización.

6.2 Proceso de gestión de controles.
Este se lleva a cabo en tres niveles los cuales son:

- Primer nivel Organización: proporciona la información rentable y eficiente, soluciones tecnológicas consistentes con los objetivos de la organización.
- Segundo nivel Misión / Procesos Empresariales: establece los requisitos de Seguridad de la Información, establece una arquitectura empresarial para facilitar la asignación de controles de seguridad a los sistemas de información
- Tercer nivel Sistemas de información: el Marco de Gestión de Riesgos (RMF) es el principal medio para abordar el nivel tres debido a que jerarquiza la gestión del riesgo.

6.3 Marco de Gestión de Riesgos.

- Paso 1 Clasificar por categorías el sistema de información.
- Paso 2 Seleccionar la línea base del control de seguridad.
- Paso 3 Implementación de controles de seguridad documentando el diseño, desarrollo y detalles de su implementación.
- Paso 4 Evaluación de los controles de seguridad para determinar el impacto de estos.
- Paso 5 Autorización de la operación del sistema de información basado en la determinación de los riesgos.
- Paso 6 Monitorear de manera continua la operación de los controles, para determinar su efectividad.

Antes de considerar el tratamiento y seguimiento de los riegos, el área de informática decidirá los criterios y restricciones para determinar la criticidad y aceptación de los riesgos. Es decir, un riesgo puede ser aceptado si, por ejemplo, se determina que el costo de su tratamiento no es rentable para la organización o el impacto de este afecta de manera considerable a la organización.

Cabe mencionar que para la aceptación de los riegos debe ser de manera consciente y objetiva siempre y cuando cumplan las políticas y los criterios de la organización.

La evaluación de la eficacia del sistema de gestión de Seguridad de la Información lo determina la organización ya que delimita a qué es necesario dar seguimiento, los métodos, medición, análisis, evaluación y quien debe hacerlo.

De acuerdo con la información obtenida previamente con las políticas existentes dentro del área se determinó que las principales mejoras serían en:

- Controles físicos.
- Controles lógicos.
- Controles administrativos.

6.4 Controles según la Norma ISO 27002.
Con base a los controles establecidos en la Norma ISO 27002 se hizo una extracción, algunos de ellos ya son implementados, sin embargo, para reforzar la seguridad se implementarán más controles dentro del área.

Tabla 22: controles.

Políticas para la Seguridad de la Información	Control Un conjunto de políticas para la Seguridad de la Información debe ser definido, aprobado por la dirección, publicado y comunicado a los empleados y partes externas relevantes.
Revisión de las políticas para la Seguridad de la Información	Control Las políticas de la Seguridad de la Información deben revisarse a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.
Roles y responsabilidades en Seguridad de la Información	Control Todas las responsabilidades en Seguridad de la Información deben ser definidas y asignadas.
Segregación de tareas	Control Las funciones y áreas de responsabilidad deben segregarse para reducir la posibilidad de que se produzcan modificaciones no autorizadas o no intencionadas o usos indebidos de los activos de la organización.
Política de dispositivos móviles	Control Se debe adoptar una política y unas medidas de seguridad adecuadas para la protección contra los riesgos de la utilización de dispositivos móviles.
Términos y condiciones del empleo	Control Como parte de sus obligaciones contractuales, los empleados y contratistas deben establecer los términos

	y condiciones de su contrato de trabajo en lo que respecta a la Seguridad de la Información, tanto hacia el empleado como hacia la organización.
Concienciación, educación y capacitación en Seguridad de la Información	Control Todos los empleados de la organización y, cuando corresponda, los contratistas, deben recibir una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo.
Inventario de activos	Control Los activos asociados a la información y a los recursos para el tratamiento de la información deben estar claramente identificados y debe elaborarse y mantenerse un inventario.
Propiedad de los activos	Control Todos los activos que figuran en el inventario deben de tener un propietario.
Devolución de los activos	Control Todos los empleados y terceras partes deben devolver todos los activos de la organización que estén en su poder al finalizar su empleo, contrato o acuerdo.
Manipulación de la información	Control Debe desarrollarse e implantarse un conjunto adecuado de procedimientos para la manipulación de la información, de acuerdo con el esquema de clasificación adoptado por la organización.
Política de control de acceso	Control Se debe establecer, documentar y revisar una política de control de acceso basada en los requisitos de negocio y de Seguridad de la Información.
Acceso a las redes y a los servicios de red	Control Únicamente se debe proporcionar a los usuarios el acceso a las redes y a los servicios en red para cuyo uso haya sido específicamente autorizados.
Registro y baja de usuarios	Control Debe implantarse un procedimiento formal de registro y retirada de usuarios que haga posible la asignación de los derechos de acceso.
Provisión de acceso de	Control

usuario	Debe implantarse un procedimiento formal para designar o remover los derechos de acceso para todos los tipos de usuarios de todos los sistemas y servicios.
Gestión de privilegios de acceso	Control La asignación y el uso de privilegios de acceso debe estar restringida y controlada.
Revisión de los derechos de acceso de usuario	Control Los propietarios de los activos deben revisar los derechos de acceso de usuario a intervalos regulares
Retirada o reasignación de los derechos de acceso	Control Los derechos de acceso de todos los empleados y terceras partes, a la información y a los recursos de tratamiento de la información deben ser retirados a la finalización del empleo, del contrato o del acuerdo, o ajustados en caso de cambio.
Restricción del acceso a la información	Control Se debe restringir el acceso a la información y a las funciones de las aplicaciones, de acuerdo con la política de control de acceso definida.
Procedimientos seguros de inicio de sesión	Control Cuando así se requiera en la política de control de acceso, el acceso a sistemas y al as aplicaciones se debe controlar por medio de un procedimiento seguro de inicio de sesión.
Sistema de gestión de contraseñas	Control Los sistemas para la gestión de contraseñas deben ser interactivos y establecer contraseñas seguras y robustas.
Controles físicos de entrada	Control Las áreas seguras deben estar protegidas mediante controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado.
Protección contra las amenazas externas y externas ambientales	Control Se debe de diseñar y aplicar una protección física contra desastres naturales, ataques provocados por el hombre o accidentes.
Emplazamiento y protección de equipos	Control Los equipos deben situarse o protegerse de forma que se reduzcan los riesgos de las amenazas y los riesgos ambientales, así como las oportunidades de que se

	produzcan accesos no autorizados.
Instalaciones de suministro	Control Los equipos deben estar protegidos contra fallos de alimentación y otras alteraciones causadas por fallos en las instalaciones de suministro.
Seguridad del cableado	Control El cableado eléctrico y telecomunicaciones que transmite datos o que sirve de soporte a los servicios de información debe estar protegido frente a interceptaciones, interferencias o daños.
Mantenimiento de los equipos	Control Los equipos deben recibir un mantenimiento correcto que asegure su disponibilidad y su integridad continuas.
Equipo de usuario desatendido	Control Los usuarios deben asegurarse de que el equipo desatendido tiene la protección adecuada.
Política de puesto de trabajo despejado y pantalla limpia	Control Debe de adoptarse una política de puesto de trabajo despejado de papeles y medios de almacenamiento y una política de pantalla limpia para los recursos de tratamiento de la información.
Copias de Seguridad de la Información	Control Se deben realizar copias de Seguridad de la Información, del software y del sistema y se deben verificar periódicamente de acuerdo con la política de copias de seguridad acordada.
Restricción en la instalación de software	Control Se debe establecer y aplicar reglas que rijan la instalación de software por parte de los usuarios.
Controles de red	Control Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y aplicaciones.
Acuerdos de confidencialidad o no revelación	Control Deben identificarse, documentarse y revisarse regularmente los requisitos de los acuerdos de confidencialidad o no revelación.
Notificación de los eventos de Seguridad de la Información	Control Los eventos de Seguridad de la Información se deben notificar por los canales de gestión adecuados lo antes

	posible.
Notificación de puntos débiles de la seguridad	Control Todos los usuarios o terceras partes y servicios de información deben ser obligados a notar y notificar cualquier punto débil que observen o que sospechen que exista en los sistemas o servicios.
Evaluación y decisión sobre los eventos de seguridad de información	Control Los eventos de Seguridad de la Información deben ser evaluados y debe decidirse si se clasifican como incidentes de Seguridad de la Información.
Respuesta a incidentes de Seguridad de la Información	Control Los incidentes de Seguridad de la Información deben ser respondidos de acuerdo con los procedimientos documentados.
Cumplimiento de las políticas y normas de seguridad	Control Los directivos deben asegurarse de que todos los procedimientos de dentro de su área de responsabilidad se realizan correctamente con el fin de cumplir las políticas y normas de seguridad y cualquier otro requisito de seguridad aplicable.

Fuente: ISO/IEC. (2013). INTERNATIONAL STANDARD ISO/IEC 27002 (2nd ed.).

Para la implantación de un sistema de controles habrá que definir:

- Gestión de sistemas de información: políticas, pautas y normas técnicas que sirvan de base para el diseño y la implantación de los sistemas información y de los controles correspondientes.
- Administración de sistemas: controles sobre la actividad de los centros de datos y otras funciones de apoyo al sistema, incluyendo la administración de las redes.
- Seguridad: incluye las tres clases de controles fundamentales implantados en el software del sistema: integridad del sistema, confidencialidad (control del acceso) y disponibilidad.

6.5 Controles Existentes vs Controles Propuestos.

En la siguiente tabla se hace un comparativo entre los controles existentes dentro del área y los que se proponen.

Tabla 23: comparación de controles.

Control	Controles implementados	Controles por implementar
Políticas para la Seguridad de la Información	✗	✗

Control	Controles implementados	Controles por implementar
Revisión de las políticas para la Seguridad de la Información		✗
Roles y responsabilidades en Seguridad de la Información	✗	
Segregación de tareas		✗
Política de dispositivos móviles		✗
Términos y condiciones del empleo		✗
Concienciación, educación y capacitación en Seguridad de la Información		✗
Inventario de activos	✗	
Propiedad de los activos	✗	
Devolución de los activos	✗	
Manipulación de la información		✗
Política de control de acceso		✗
Acceso a las redes y a los servicios de red	✗	
Registro y baja de usuarios	✗	
Provisión de acceso de usuario		✗
Gestión de privilegios de acceso		✗
Revisión de los derechos de acceso de usuario		✗
Retirada o reasignación de los derechos de acceso		✗
Restricción del acceso a la información		✗
Procedimientos seguros de inicio de sesión		✗
Sistema de gestión de contraseñas		✗
Controles físicos de entrada		✗

Control	Controles implementados	Controles por implementar
Protección contra las amenazas externas y externas ambientales		✗
Emplazamiento y protección de equipos		✗
Instalaciones de suministro		✗
Seguridad del cableado		✗
Mantenimiento de los equipos	✗	
Equipo de usuario desatendido		✗
Política de puesto de trabajo despejado y pantalla limpia		✗
Copias de Seguridad de la Información		✗
Restricción en la instalación de software		✗
Controles de red	✗	
Acuerdos de confidencialidad o no revelación		✗
Notificación de los eventos de Seguridad de la Información		✗
Notificación de puntos débiles de la seguridad		✗
Evaluación y decisión sobre los eventos de seguridad de información		✗
Respuesta a incidentes de Seguridad de la Información		✗
Cumplimiento de las políticas y normas de seguridad		✗

Fuente: elaboración propia.

Capítulo 7 Propuesta para establecer un programa de mejora de seguridad con el modelo PDCA (Planificar-Hacer-Verificar-Actuar) dentro del área de informática del Municipio de Ecatepec de Morelos.

7.1 ¿Qué es el ciclo PDCA?

Se denomino ciclo PDCA por las siglas Planificar (Plan), Hacer (Do), Verificar (Check) y Actuar (Act), este ciclo se conoce también como Ciclo de Deming o Ciclo de Mejora Continua.

Esta metodología describe los cuatro pasos para llevar a cabo una mejora continua, teniendo como objetivo el mejoramiento de la calidad de los procesos, previsión y eliminación de riesgos, etc.

Ilustración 1: ciclo PDCA (plan, hacer, verificar y actuar).

Fuente: elaboración propia.

7.2 Propuesta.

Tabla 24: implementación de PDCA.

Planificar	Hacer	Verificar	Actuar
Se observa que existe personal que tiene acceso a los sistemas de información. Estos no se encuentran	Se implementarán políticas gestionar el acceso a los sistemas de información.	Se realizará el seguimiento de la política implementada para verificar que sea	Se realizará un análisis de información sobre la política implementada.

Planificar	Hacer	Verificar	Actuar
previamente autorizados.	Se capacitará al personal respecto a la política del acceso al sistema de información.	aplicada correctamente.	Para medir los impactos que esta tuvo sobre los accesos no autorizados.
Se observa que los empleados del área de informática no bloquean su equipo cuando estos se alejan de su área de trabajo.	Se implementa la política de bloqueo de equipos donde se establece el procedimiento cuando el empleado se aleje de su equipo de trabajo. Se configura el equipo para ser bloqueado en un intervalo de tiempo determinado.	Se realizará un seguimiento a la política implementada, reportando el equipo que no se encuentre bloqueado por inactividad.	Se medirá el impacto de la política implementada y si estos son positivos se seguirá implementada, si el impacto es negativo se repetirá el ciclo.
Se observa una mala aplicación de controles lógicos.	Se implementa política de controles lógicos para acceso al sistema de información.	Se restringirán los accesos a la información dependiendo el nivel del empleado.	Se medirá el impacto de la política implementada y si estos son positivos se seguirá implementada, si el impacto es negativo se repetirá el ciclo.
Se observa el acceso a redes sociales.	Se establecerá una política con y el procedimiento para bloquear el uso de redes sociales.	Se implementará un bloqueo de URL de las redes sociales.	Se realizarán pruebas en los distintos dispositivos para verificar que no se tiene acceso a redes sociales.
Se observa medios de almacenamiento físicos expuestos a personas externas al área.	Implementar políticas y procedimientos que se aplicarán hacia las personas que manipulen medios de	Se evaluará si con la aplicación de la política se tiene un mayor control de los medios de almacenamiento y si estos no se encuentran	Derivada de la evaluación se establecerá si se sigue aplicando la política o se aplica nuevamente el ciclo y se crea una nueva política.

Planificar	Hacer	Verificar	Actuar
	almacenamiento físicos.	expuestos a externos.	
Se observa un incorrecto uso de controles físicos para ingresar al área (Acceso de personas ajenas del área al equipo de cómputo).	Se establecerá una política con procedimiento para acceder al área.	Se pedirá un registrarse en una bitácora a toda aquella persona externa ajena al área o a la organización.	Se verificará cada que sea necesario el uso de la bitácora y el registro de personas externas.
Se observa problemas de conectividad en la red interna de la organización.	Se implementarán los nuevos procesos y procedimientos a seguir para tener una mejor gestión de quien puede manipular las redes en caso de que falle la conectividad de esta, dichos procesos tendrán que estar apegados a las políticas de la organización.	Pasado un periodo de 6 meses se evaluará que los procesos y procedimiento, todo esto para prevenir que personas ajenas a la organización tengan acceso a la red de la organización y poder prevenir el robo o pérdida de dicha información.	Una vez que fueron evaluados los procesos y procedimientos se tomará la decisión de implementarlos definitivamente o de volver a implementar nuevos procesos y procedimientos todo esto con el fin de tener una mejora continua en la gestión de la información.
Se observa problemas de conectividad con el servicio de internet.	Se contará con el contrato de servicios del proveedor de internet. Se verificará que este proporcione soporte en caso de fallo del servicio.	Se establecerán pruebas de conexión de internet.	Si las pruebas de conexión no son satisfactorias se buscará la mejora del servicio.
Se observa diversos problemas con el software (desactualización y licencias vencidas).	Se llevará un control del software utilizado dentro del área. Se planificará un calendario semestral para el mantenimiento preventivo y	Se llevará a cabo las revisiones de las licencias y que estas estén activadas.	Se registra en un archivo electrónico los equipos, software utilizado y las fechas de activación y terminación de las licencias.

Planificar	Hacer	Verificar	Actuar
	correctivo de los equipos.		
Se observa fallo de hardware dentro del área.	Se planificará un calendario semestral para el mantenimiento preventivo y correctivo de los equipos. Se contará con un inventario del hardware.	Se realizará el seguimiento del funcionamiento del hardware.	Una vez que fueron implementados los calendarios y mantenimientos se evaluará el rendimiento del hardware.
Se observa que el edificio donde se encuentra el área es propenso a sufrir bloqueos de acceso por parte de terceras personas.	Se implementarán planes que permitan la rápida reacción del personal. Se determinará el personal crítico y los recursos que estos necesitan para seguir con la operación.	Se probarán los planes que simulan una contingencia en este caso el bloqueo de accesos.	Se medirán los tiempos de respuesta del área en contingencia.
Se observa que el edificio es propenso a sufrir una interrupción del servicio eléctrico.	Se implementarán planes que permitan la rápida reacción del personal. Se determinará el personal crítico y los recursos que estos necesitan para seguir con la operación.	Se probarán los planes que simulan una contingencia.	Se medirán los tiempos de respuesta del área cuando se encuentren en contingencia.
Se observa que el edificio es propenso a sufrir una crisis de seguridad debido a que se encuentra.	Se implementarán planes que permitan la rápida reacción del personal. Se determinará el personal crítico y los recursos que estos necesitan	Se probarán los planes que simulan una contingencia.	Se medirán los tiempos de respuesta del área cuando se encuentren en contingencia.

Planificar	Hacer	Verificar	Actuar
	para seguir con la operación.		
Se observa que no existen políticas o estas están obsoletas.	En el encargado de seguridad en conjunto con todos los encargados del área evaluaran, definirán y establecerán un conjunto de políticas y sanciones salvaguarden la seguridad informática y los activos de información. Se capacitarán a los empleados en materia de seguridad informática. Se comunicarán las políticas a todos los empleados del área.	Se verificará que las políticas hayan sido comunicadas a los empleados. Se llevará un control en materia de capacitación d seguridad informática es decir calendarios, horas de capacitación, temario, etc.	Se llevará a cabo una actualización anual de las políticas.
Se observa que no hay sanciones establecidas para el incumplimiento de las políticas.			
No se observa la existencia de una evaluación e identificación de riesgos y amenazas.	En el encargado de seguridad en conjunto con todos los encargados del área ya sea con ayuda de un externo / consultor realizaran, evaluaran, identificaran y trataran los riesgos y amenazas a los que se ven expuestos.	Se realizará un informe con los resultados obtenidos con la evaluación e identificación de los riesgos y amenazas.	Se dará un tratamiento adecuado a los riesgos y amenazas a adecuado, ya sea transfiriéndolos a un tercero o llevando el tratamiento ellos mismos.
No se observa un tratamiento contra las amenazas existentes.			

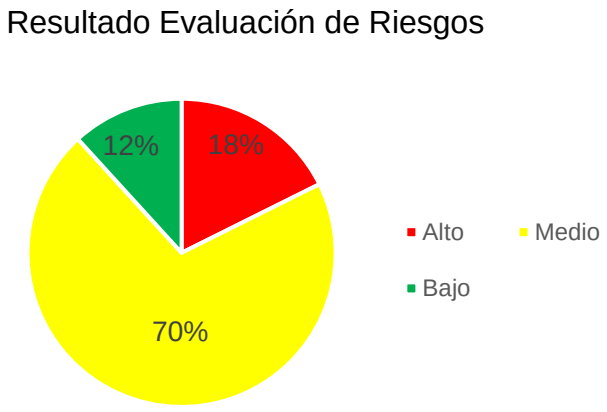
Fuente: elaboración propia.

Capítulo 8 Resultados

Como resultado de la presente tesis, se identificaron los siguientes riesgos a los que se ve expuesto de área de informática del municipio de Ecatepec de Morelos, estos se fueron clasificados según su nivel de riesgo (alto, medio, bajo).

Dando como resultado la siguiente gráfica:

Ilustración 2: resultado de evaluación de riesgos.



Fuente: elaboración propia.

El 70% de los riesgos fueron clasificados de acuerdo con las metodologías utilizadas en la categoría “medio” de los cuales los resaltan los siguientes debido a su puntaje obtenido.

- Fallo, desactualización o defecto del software
- Mala aplicación de controles lógicos
- Bloqueo a los accesos del edificio

Sin embargo, dentro de este análisis se obtuvieron tres riesgos con la categoría “alto”, se recomienda la rápida mitigación ya que pueden derivar en pérdidas de información.

- Los controles físicos de acceso no están actualizados (Acceso de personas ajenas del área al equipo de cómputo)
- Acceso no autorizado a los sistemas informáticos
- No existe una evaluación e identificación de riesgos y amenazas

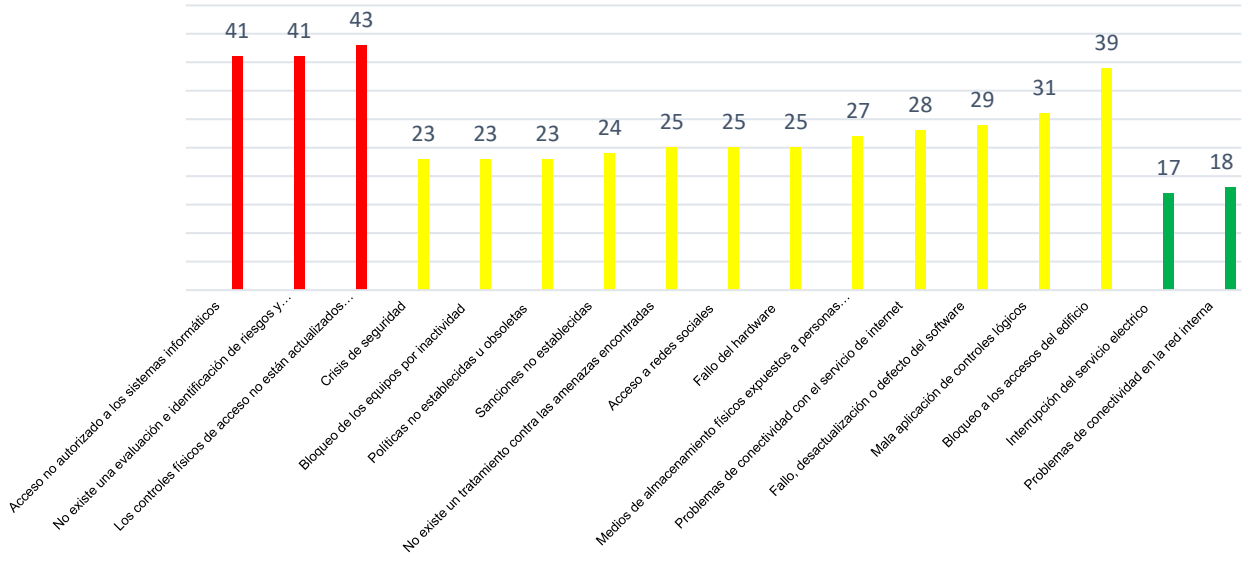
8.1 Listado de los riesgos encontrados.

Tabla 25: riesgos.

Riesgo	Categoría
Acceso no autorizado a los sistemas informáticos	41
No existe una evaluación e identificación de riesgos y amenazas	41
Los controles físicos de acceso no están actualizados (Acceso de personas ajenas del área al equipo de cómputo)	43
Crisis de seguridad	23
Bloqueo de los equipos por inactividad	23
Políticas no establecidas u obsoletas	23
Sanciones no establecidas	24
No existe un tratamiento contra las amenazas encontradas	25
Acceso a redes sociales	25
Fallo del hardware	25
Medios de almacenamiento físicos expuestos a personas externas	27
Problemas de conectividad con el servicio de internet	28
Fallo, desactualización o defecto del software	29
Mala aplicación de controles lógicos	31
Bloqueo a los accesos del edificio	39
Problemas de conectividad en la red interna	18
Interrupción del servicio eléctrico	17

Fuente: evaluación propia.

Ilustración 3: análisis de resultados.



Fuente: elaboración propia.

Conclusiones

Tras el levantamiento de información, la presente tesis tuvo como objetivo demostrar los fallos de seguridad a los cuales se ve expuesta la organización.

Se tomo en cuenta las políticas, controles y recursos con la que esta contaba al momento de realizar la recopilación de información.

Así pues, la participación de este trabajo finalizo con:

- Actualización y diseño de las políticas de seguridad.
- Definición de sanciones al incumplimiento de las políticas de seguridad
- Definición y delimitación de roles y responsabilidades.
- Sugerencia de listado de controles para el reforzamiento de la seguridad basados en la Norma ISO 27002.
- Uso de las metodologías OCTAVE y PDCA para identificar los riesgos de la organización.

Por este motivo, la Seguridad de la Información no solo debe limitarse a recursos de TI sino a toda la organización y sus recursos (personas, hardware, software, etc.), aplicando, comprendiendo, capacitando y concientizando de su importancia a todo el personal, desde la alta dirección hasta los responsables de la operación del día a día.

Bibliografía

Baca, G. (2016). Introducción a la seguridad informática. México: Grupo Editorial Patria.

Beekman, G. (2005). Introducción a la informática (6th ed.). Madrid, España: Pearson Educación de México, S.A. de C.V.

Caralli, R. (2007). Introducing OCTAVE Allegro. Pittsburgh, Pa.: Carnegie Mellon University, Software Engineering Institute.

Costas, J. (2010). Seguridad Informática (1st ed.). Madrid, España: RA-MA.

Costas, J. (2011). Mantenimiento de la seguridad en sistemas informáticos (1st ed.). Starbook Editorial, S.A.

Fernández, C., & Piattini, M. (2012). Modelo para el gobierno de las TIC basado en las normas ISO (1st ed.). España: AENORediciones.

Gómez, Á. (2006). Enciclopedia de la Seguridad Informática (2nd ed.). Madrid, España: RA-MA.

ISACA (2018), COBIT 2019 Framework Governance and Management Objectives. Schaumburg, USA. Obtenido de https://www.isaca.org/bookstore/bookstore-cobit_19-digital/wcb19fgm

ISO/IEC. (2005). Norma internacional ISO/IEC 27001 Tecnología de la información-Técnicas de seguridad – Sistemas de Gestión de la información (SGSI) - Requisitos (1st ed.). Madrid, España.

ISO/IEC. (2013). International standard ISO/IEC 27002 (2nd ed.). Ginebra, Suiza.

Laudon, K., Laudon, J., Vidal Romero Elizondo, A., & Solares Soto, P. (2012). Sistemas de información gerencial (12th ed.). DF, México: Pearson.

Norma internacional ISO / IEC 27000. (2018). [e-book] (5ª ed.). Vernier, Ginebra, Suiza. Obtenido de https://standards.iso.org/ittf/PubliclyAvailableStandards/c073906_ISO_IEC_27000_2018_E.zip

Russell, S., & Norvig, P. Artificial intelligence (2nd ed., p. 1179). Madrid: Pearson.

Solís, G. (2002). Reingeniería de la auditoría informática. México: Trillas.

U.S. Dept. of Commerce, National Institute of Standards and Technology. (1990). NIST. Gaithersburg, Md.

ISOTools. (21 Febrero 2019). Beneficios de normas ISO. 8 octubre 2021, de PLATAFORMA TECNOLÓGICA PARA LA GESTIÓN DE LA EXCELENCIA Sitio web: https://www.isotools.org/2019/02/21/beneficios-de-normas-iso/

CTMA CONSULTORES. (17 AGOSTO 2020). Cómo implementar ISO 27001 en tu empresa. 08 OCTUBRE 2021, de CTMA CONSULTORES Sitio web: https://ctmaconsultores.com/como-implementar-iso-27001/

ISOTOOLS. (20 FEBRERO 2015). Blog Calidad y Excelencia. 8 OCTUBRE 2021, de PLATAFORMA TECNOLÓGICA PARA LA GESTIÓN DE LA EXCELENCIA Sitio web: https://www.isotools.org/2015/02/20/en-que-consiste-el-ciclo-phva-de-mejora-continua/