TECNOLÓGICO DE ESTUDIOS SUPERIORES DE CUAUTITLAN IZCALLI

“IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD DE INFORMACIÓN BASADOS EN ISO 27001”

QUE PARA OBTENER EL GRADO DE:
MAESTRO EN TECNOLOGÍAS DE LA INFORMACIÓN

PRESENTA:

LICENCIADO ISRAEL GUARNEROS MORENO

DIRECTOR DE TESIS:
DR.ESTEBAN CONTRERAS GONZALEZ

CUAUTITLAN IZCALLI EDO. DE MEXICO AGOSTO 2023

"2023. Año del Septuagésimo Aniversario del Reconocimiento del Derecho al Voto de las Mujeres en México".

Cuautitlán Izcalli, México a 03 de agosto de 2023.
TESCI/DIDT/76/VIII/23.
Asunto: CEREMONIA DE TITULACIÓN

DIRECCIÓN ACADÉMICA
COORDINACIÓN DE POSGRADO

MTRA. MARTHA EVA PAREDES ORTEGA
DIRECTORA ACADÉMICA

Por este conducto me permito informarle que la ceremonia de Titulación para obtener el Título Profesional de Maestro en Tecnologías de la Información mediante la opción: "TESIS" del C. LIC. ISRAEL GUARNEROS MORENO No. de Control 213101007, ha sido programada para el día 10 de agosto de 2023 a las 14:00 horas. Lugar: Se llevará a cabo en el Auditorio B.

Fungirán como sinodales:

PRESIDENTE	DR. ESTEBAN CONTRERAS GONZÁLEZ	Ced. Prof. 9997490
SECRETARIA	M. EN T.I. VIRIDIANA JIMÉNEZ MARTÍNEZ	Ced. Prof. 12986826
VOCAL	M. EN A. ELVA BERNAL RODRÍGUEZ	Ced. Prof. 10134583
SUPLENTE	M. EN A. ERIKA EMILIA CANTERA	Ced. Prof. 9619909

ATENTAMENTE

TECNOLÓGICO DE ESTUDIOS SUPERIORES DE CUAUTITLÁN IZCALLI
UNIDAD DE POSGRADO

MTRA. ERIKA EMILIA CANTERA
COORDINACIÓN DE POSGRADO

c.c.p. Dra. Maribel Chávez Hernández, Subdirectora de Apoyo y Desarrollo Académico
Mtra. Teresa Ramírez Mora, Subdirectora de Estudios Profesionales
Mtra. Rocío Ortega Jiménez, División de Ingeniería en Sistemas Computacionales
Ing. Adriana Ivett del Olmo Saldaña, División de Ingeniería Mecatrónica
Dr. Esteban Contreras González
Mtra. Elva Bernal Rodríguez
Mtra. Viridiana Jiménez Martínez
Área de Titulación y Servicio Social
Lic. Israel Guarneros Moreno

ÍNDICE

INTRODUCCION

En cualquier organización o entidad laboral es imprescindible el uso de los sistemas de información ya que se manejan grandes cantidades de información y el uso de equipo informático es impredecible, por lo cual todo esto puede provocar la aparición de vulnerabilidades poniendo en riesgo a toda la red computacional de la organización o institución.

Por tal razón se debe de buscar la mejor manera de resguardar la información sensible de la organización y protegerla de ataques internos y externos o desastres naturales, por esta razón es de suma importancia elaborar políticas de seguridad de información que detallen la manera en donde se establezcan las pautas a seguir por cada colaborador, claro que para ello el personal debe estar involucrado y tener capacitaciones de concientización para que tenga un sentimiento de pertenencia en la empresa , institución u organización y se responsabilice de los activos entregados para el desarrollo de sus actividades.

El colegio nacional de educación es una institución educativa que se dedica a la impartición de bachillerato tecnológico y también ofrece cursos de extensión educativa, su departamento de servicios es encargado de gestionar las inscripciones, reinscripciones, matriculación, calificaciones, altas, bajas y demás tramites que el alumno requiera académicamente pero no cuenta con un sistema de seguridad para la información que en ella procesa.

Es por ello que la realización de este trabajo tiene como objetivo la Implementación de las políticas de seguridad de la información basadas en ISO

27001 según las necesidades de este departamento para la continuidad de sus actividades sin ningún tipo de inconvenientes que tengan que ver con seguridad informática.

Se debe describir de manera clara por qué y para que se busca proteger y de igual manera concientizar a todo el personal para el cumplimiento de las políticas de seguridad informática.

2. CONTEXTUALIZACION

2.1 CONTEXTUALIZACIÓN DE LA INSTITUCION

Nombre de la institución: Colegio Nacional de Educación Profesional Técnica

Ubicación

Edomex

Giro: educación

Misión:

Formar capital Humano de clase mundial en el campo tecnológico y de servicios Para el desarrollo Del estado de México

Visión:

Trabajando en grande nos consolidamos Como la institución pública líder en la Formación de profesionales técnicos-bachilleres, en servicios tecnológicos y de capacitación en el país

2.2 CONTEXTUALIZACION DEL DEPARTAMENTO

Nombre del departamento:

Control escolar.

Objetivo del departamento:

Brindar información y documentación que tienen que ver

Con la historia académica de los alumnos, ofreciendo de esta manera trámites y servicios conforme al reglamento escolar vigente en ese momento en la institución educativa.

Procesos generales que desarrollan:

Planeación, control, evaluación con actividades que estén relacionadas con Prestaciones de servicios escolares

Supervisar que se cumpla la normatividad que emiten las autoridades de la institución

Reinscripción. Inscripción, formación de expedientes de cada uno de los alumnos, equivalencias, bajas, cambios de plantel

Coordinar las certificaciones y titulaciones de los alumnos conforme a los Protocolos establecidos en la institución.

3. JUSTIFICACIÓN

La norma ISO 27001 aporta un Sistema de Gestión de la Seguridad de La Información (SGSI), consistente en medidas orientadas a proteger la información.

Permite que las organizaciones se pueden certificar.

ISO 27001 se ha convertido en la principal norma a nivel mundial para la Seguridad de la información.

Se puede aplicar en cualquier tipo de organización

La maestría en tecnologías de la información nos permite tener un conocimiento más integral porque:

- Se trabaja en áreas de
- Administración
- Matemáticas
- Gestión de la información
- Desarrollo de software
- Redes y telecomunicaciones
- Al ser más integral permite desarrollar e implementar proyectos de ingeniería y administración o la combinación de ambos

4. OBJETIVOS

4.1 OBJETIVO GENERAL

Implementar procesos de seguridad informática bajo el estándar ISO 27001 dentro de los activos sensibles, que permitan la continuidad de las operaciones dentro Del departamento de servicios educativos maximizando la confiabilidad, integridad disponibilidad y no repudio de la información

4.2 OBJETIVOS ESPECÍFICOS

- Identificar los activos sensibles del departamento de servicios educativos
- Listar las principales amenazas a los activos críticos del Departamento de servicios educativos
- Desarrollar las políticas de seguridad informática basadas en la norma ISO 27001 que se acoplen a las necesidades del departamento de servicios educativos
- Desarrollar el plan de recuperación desastres basado en el estándar ISO 27001para el departamento de servicios educativos
- Implementar los procesos de seguridad informática en el departamento de servicios educativos
- Capacitar al personal activo en la ejecución de los procesos de seguridad informática

5. METODOLOGIA

5.1Tipo de investigación

1. Mixta (cualitativa y cuantitativa)
2. Se relaciona con la pregunta de investigación
3. Se relaciona con los objetivos
4. y se desea comprobar una realidad (la vulnerabilidad ante ataques Informáticos)

5.2 Variables a medir

¿Cómo se podrá saber cuánto ha disminuido los ataques después de la Implementación?

Se medirá mediante un sistema de detección de intrusos (IDS) como por ejemplo:

HIDS (HostIDS)

(HIDS, Sistema de detección de intrusos en un Host. Busca detectar anomalías que indican un riesgo potencial, revisando las actividades en la máquina (host). Puede tomar medidas protectoras

NIDS (NetworkIDS)
istema de detección de intrusos en una Red. Busca detectar anomalías que inicien un riesgo potencial, tales como ataques de denegación de servicio, escaneadores

De puertos o intentos de entrar en un ordenador, analizando el tráfico en la red en tiempo real. Para ello, analiza todos los paquetes, buscando en ellos patrones sospechosos. Los NIDS no sólo vigilan el tráfico entrante, sino también el saliente o el tráfico local, ya que algunos ataques podrían ser iniciados desde el propio sistema protegido.

IDS basados en firmas

Los IDS basados en firmas supervisan todos los paquetes de la red y los comparan con la base de datos de firmas, que son patrones de ataque preconfigurados y predeterminados. Funcionan de forma similar al software antivirus.

IDS basados en anomalías

Estos IDS monitorean el tráfico de red y lo comparan con una línea de base establecida. La línea base determina lo que se considera normal para la red en términos de ancho de banda, protocolos, puertos y otros dispositivos, y el IDS alerta al administrador de todo tipo de actividad inusual.

IDS Pasivo

Este sistema IDS realiza el sencillo trabajo de detección y alerta. Simplemente alerta al administrador de cualquier tipo de amenaza y bloquea la actividad en cuestión como medida preventiva.

Identificación reactiva

Detecta actividad malintencionada, alerta al administrador de las amenazas y también responde a esas amenazas.

5.3 Técnicas para recabar información

- Entrevistas
- Cuestionarios
- Reuniones
- Observación
- Revisión de documentación
- Pruebas de penetración con IDS

5.4 Población y muestra

La población total la conforman todos los empleados que conforman los departamentos que integran a la institución educativa

- Dirección
- Departamento finanzas
- Servicios educativos
- Coordinación tecnológica y de sistemas
- Coordinación académica

Cuya población se totaliza en 85 empleados

5.5 Muestra:

Los criterios a tomar en cuenta para la selección dentro de la población serán:

- Directivos del departamento ya que poseen amplio conocimiento de los procesos y actividades que deben realizar los operarios del área y mantienen un rol de ejecutor en la toma de decisiones

- Operario. Es el que realiza o manipula información para llevar a cabo las actividades que su rol exige

- Se entrevistara y encuestara aleatoriamente a un total de 30 empleados ya que con esa muestra se puede lograr una apreciación muy real de la situación actual al ser personas que cumplen un papel relevante dentro de la institución

5.6 Estado de resultados

Mitigación de Vulnerabilidades en los sistemas informáticos

Integridad, confiabilidad, y disponibilidad de la información de los alumnos

Y personal administrativo y docente en general.

6. ESTADO DEL ARTE

1. Omar Javier Solano Rodríguez, Domingo García Pérez de Lema, Juan Jesús Bernal. (2016). the information system and computer security mechanisms in the SMEs. Colombia: casa editorial el tiempo

Objetivo:

Determinar empíricamente cómo la participación del usuario, los factores Tecnológicos y la gestión organizacional contribuyen al diseño y desempeño de los controles al sistema de información (SI) de la pequeña y mediana empresa (pyme).el uso de herramientas tecnológicas, el diseño y desarrollo de los controles que se usan para prevenir y detectar el riesgo informático

2. Jorge Ramio Aguirre, Josep María MiretBiosca. (2006). Seguridad Informática y Criptografía. España: RA-MA Editorial

Objetivo

Protección de la disponibilidad de la información mediante sistemas tolerantes a fallos, estrategias de recuperación de sistemas y copias de seguridad, planes de contingencia, utilización de las firmas electrónicas y los certificados digitales,elección adecuada de cortafuegos, creación de una red privada virtual, protecciones ante el malware, sistemas de detección y prevención de intrusiones.

Si nos atenemos a la definición de la Real Academia de la Lengua española, seguridad es la “cualidad de seguro”. Buscamos ahora seguro y obtenemos “libre y exento de todo peligro, daño o riesgo”. A partir de estas definiciones no podríamos aceptar que seguridad informática es “la cualidad de un sistema informático exento de peligro”, por lo que habrá que buscar una definición más apropiada. Algo básico:

La seguridad no es un producto, sino un proceso. Por lo tanto, podríamos aceptar que una primera definición más o menos aceptable de seguridad informática sería: Un conjunto de métodos y herramientas destinados a proteger la información

Y por ende los sistemas informáticos ante cualquier amenaza, un proceso en el cual

Participan además personas. Concienciarlas de su importancia en el proceso será algo crítico. La seguridad informática no es un bien medible, en cambio si podríamos desarrollar diversas herramientas para cuantificar de alguna forma nuestra inseguridad informática.

3. Martha Irene Romero Castro Grace Liliana Figueroa Morán Denisse Soraya Vera

Navarrete José Efraín Álava Cruzatty Galo Roberto Parrales Anzures Christian José

Álava Mero Ángel Leonardo Murillo Quimiz Miriam Adriana Castillo Merino. (2018). INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE

VULNERABILIDADES. Ecuador: Editorial Área de Innovación y desarrollo.

Objetivo principal

Conocer los diversos conceptos de la seguridad informática Clasificación de la seguridad informática

Lo que debe contemplar la seguridad se puede clasificar en tres partes como son los siguientes

: • Los usuarios

• La información, y

• La infraestructura Los usuarios son considerados como el eslabón más débil de la cadena, ya que a las personas es imposible de controlar, un usuario puede un día cometer un error y olvidar algo o tener un accidente y este suceso puede echar a perder el trabajo de mucho tiempo, en muchos casos el sistema y la información deben de protegerse del mismo usuario. La información se considera como el oro de la seguridad informática

Ya que es lo que se desea proteger y lo que tiene que estar a salvo, en otras palabras, se le dice que es el principal activo. Por último, está la infraestructura esté

Puede ser uno de los medios más controlados, pero eso no implica que sea el que corre menos riesgos, siempre dependerá de los procesos que se manejan. Se deben de considerar problemas complejos, como los de un acceso no permitido, robo de identidad, hasta los daños más comunes, por ejemplo, robo del equipo, inundaciones, incendios o cualquier otro desastre natural que puede tener el material físico del sistema de la organización.

Los mecanismos preventivos en la seguridad informática son los más olvidados, los

Cuales son vistos como una pérdida de tiempo, la parte administrativa en la mayoría

De los casos lo ve como un costo extra, es algo parecido como por ejemplo, con los

Seguros médicos o seguros de vehículos, se puede pagar 10 años el seguro de un carro y nunca tener un accidente, en primera instancia se podrá analizar que es algo

Muy bueno, pero después en algún momento se podrá pensar que es un desperdicio

Haber pagado una cantidad 10 años y sin usarla. La definición de los mecanismos preventivos, consiste en una serie de revisiones periódicas, algunos cambios o mejoras de diferentes aspectos que pueden ser de hardware, software o de cualquier elemento involucrado en los sistemas y procesos, por eso es que las revisiones dependen de los procesos de la empresa y cada una tiene sus propios procesos. Los mecanismos preventivos en realidad son a largo plazo y por esta razón son considerados por la mayoría como una pérdida de tiempo y dinero. La mayoría de los ataques informáticos se pueden evitar o por lo menos disminuir el impacto, si se hiciera utilizando mecanismos preventivos, deficiencia de sistemas y otros problemas podrían encontrarse, evitarse y resolverse gracias a un buen trabajo durante esta etapa. La Barrera más fuerte a la que se enfrenta una empresa

Al querer aplicar los mecanismos preventivos, es la aceptación y el compromiso de todos los involucrados, hacer entender que no es una carga, es parte de los procesos y de lo que se debe hacer bien en la organización. Entre los elementos que se pueden aplicar en los mecanismos preventivos se puede mencionar a: • El respaldo de información: Es uno de los procesos más comunes que se pueden realizar en las compañías y que gozan de cierta aceptación general, las empresas entienden que los problemas con información son muy costosos, parece muy fácil pero seleccionar los mecanismos de respaldo no es tan sencillo como se analizar, se tiene que considerar los siguientes factores: Qué formatos de archivo se tienen, por ejemplo, MP3, archivos de texto, bases de 19 M.I. Romero Castro et al. Volver al índice datos y otros, las imágenes y vídeos por ejemplo, son archivos que normalmente necesitan atención especial.

• Horario de respaldo: Otro reto es a qué hora se puede hacer el respaldo, es común seleccionar las horas de menos tráfico.

• Control de los medios: El tener acceso a respaldos es algo de alto riesgo, se puede robar la información, manipular, perder, así que, el respaldo es una solución, pero también es otro problema que se debe resolver. •

- La comprensión de la información: No toda la información se puede comprimir, pero existe alguna que, sí lo necesita, así que se deben hacer las valoraciones respectivas.

4 Farias-Elinos, Ma. C, Mendoza-Díaz & L. Gómez-Velazco. (Farias-Elinos, Ma. C, Mendoza-Díaz & L. Gómez-Velazco). “Las Políticas de Seguridad como Apoyo a la Falta de Legislación Informática. México: McGraw-Hill.

Objetivos

Coordinar, planear y promover las actividades que tengan que ver con la parte de seguridad informática genera una situación que se ve reflejada en el crecimiento de

Problemas de seguridad que se presentan dentro de las instituciones, tales como intrusiones, robo de información, problemas de virus, entre otros, mejor conocidos como incidentes

Servicios de seguridad informática en las organizaciones

El ingeniero de seguridad informática tiene la función de brindar los servicios de seguridad en la organización, a través de la planeación, coordinación y administración de los procesos de seguridad informática, así como difundirla cultura de seguridad informática entre todos los miembros de la organización.

5. Omar Javier Solano Rodríguez, Domingo García Pérez de Lema, Juan Jesús Bernal. (2016). the information system and computer security mechanisms in the SMEs. Colombia: casa editorial el tiempo

Objetivo:

Determinar empíricamente cómo la participación del usuario, los factores tecnológicos y la gestión organizacional contribuyen al diseño y desempeño de los controles al sistema de información (SI) de la pequeña y mediana empresa (pyme). l, el uso de herramientas tecnológicas, el diseño y desarrollo de los controles que se usan para prevenir y detectar el riesgo informático

6. María Gabriela Hernández Pinto, Bertha Alice Naranjo Sánchez.. (2006). diseño de un plan estratégico de seguridad de información en una empresa México: Mc. Graw Hill.

Objetivo

Mantener segura su información de amenazas que pueden causarla quiebra de una empresa, mediante el diseño de un plan estratégico de seguridad de información que contribuya a disminuir los riesgos a los que está expuesta la información.

Diseño de un Plan Estratégico de Seguridad de Información en una empresa .Una vez que se hayan identificado los riesgos, el paso siguiente es analizarlos para Determinar su impacto, tomando así las posibles alternativas de solución, La mayoría de las empresas desconocen la magnitud del problema con el que se enfrentan, considerando la seguridad informática como algo secundario y prestando

Poca atención a los riesgos que en la actualidad existen, como lo son: las amenazas

Internas, una de ellas los errores humanos y las amenazas externas dentro de las cuales podemos nombrar a los virus. Para contrarrestar estos efectos de la falta de

Seguridad informática se presenta este trabajo que consiste en diseñar un plan estratégico de seguridad de información, que deberá seguir la organización en un corto, mediano y largo plazo, Importancia de la Seguridad de Información

La información es la sangre de todas las organizaciones y sin ella la empresa dejaría de funcionar principalmente si hablamos de empresas altamente automatizadas por lo que su seguridad sigue siendo un punto pendiente y por tanto el factor más determinante por el cual fracasan

7. Dussan Clavijo, Ciro Antonio. (2016). Políticas de seguridad informática. Cali, Colombia: Universidad Libre.

Objetivo

Desarrollar proyectos de seguridad informática que garanticen la integridad, disponibilidad y accesibilidad de la información. La creación de políticas de seguridad

La globalización de la economía ha exigido que las empresas implementen plataformas tecnológicas que soporten la nueva forma de hacer negocios, El ofrecer productos o servicios a través de Internet sin tomar en cuenta la seguridad informática no sólo denota negligencia, sino que constituye una invitación para que ocurran incidentes de seguridad que podrían dañar severamente la reputación y afectar los ciclos del negocio. Las vulnerabilidades2 en los sistemas de información pueden traer graves problemas. Cada vez las redes están expuestas a virus informáticos, spam, código malicioso, hackers y crackers que penetran los sistemas de seguridad. Los elementos que la seguridad

8. Rodríguez Nelly Ethel, Horacio Villa García. (2009). Seguridad Informática para alumnos de la Escuela Secundaria. . México: McGraw-Hill

Objetivo

Desarrollar una herramienta que facilite el aprendizaje de los estudiantes de la Escuela Secundaria sobre el tema Seguridad Informática creando un diseño que despierte interés en el alumnado sobre la materia de estudio y que ayude al estudiante a aprender de la práctica directa con la computadora

Durante la ejecución de las tareas escolares en la sala de computación, y Generalmente mientras utilizan las computadoras para cualquier proceso, los alumnos de la Escuela Secundaria no toman conciencia sobre los riesgos que corre

La información que se almacena en una PC, principalmente cuando se les suministran datos desde una red local, desde la red Internet o cuando transportan información a través de distintos dispositivos extraíbles. Confían en los datos que la

Computadora les ofrece, no toman las precauciones necesarias para mantener al resguardo la información que manejan, quieren guardar todo tipo de archivos (imágenes, animados, fotos, artículos, textos, videos, noticias) sin tomar en cuenta de dónde provienen esos datos y cómo deben manipularlos.

La problemática actual que aqueja a la seguridad informática junto a la problemática

De la didáctica, y a la problemática actual del contexto escolar, llevan a pensar en la posibilidad del desarrollo de un software educativo que contemple los contenidos

Curriculares de seguridad informática para atemperar algunas de las dificultades que potencian los bajos rendimientos en el proceso enseñanza-aprendizaje.

9. Felipe Bracho Carpizo, José Roberto Sánchez Soledad. (2018). el valor de la privacidad: datos personales en tiempos del panóptico. seguridad cultura de prevención para ti, 31, 59.

Objetivo

En este mundo de amenazas, en el que los usuarios finales juegan un papel estelar

(Por ser el eslabón más débil en la cadena de seguridad), el tema del control de los

Datos personales ha tomado relevancia debido a la preocupación de que las personas puedan ser controladas por medio de la información que ellas mismas

otorgan a las organizaciones y porque se ha destacado que los usuarios son el producto de las compañías, quienes lucran con la información personal de distintas

Maneras. Por lo cual, los expertos en ciberseguridad advierten de qué manera se exponen los datos personales y cómo se pueden mitigar los riesgos que ello implica.

Confidencialidad de la información El 7 de septiembre se reportó un evento catastrófico para millones de personas del país vecino del Norte. Uno de los principales burós de crédito de los Estados Unidos,

Esquifa, informó que la información de más de 145 millones de ciudadanos (incluyendo residentes del Reino Unido y Canadá) había sido comprometida en un ataque que, según las últimas investigaciones, duró más de dos meses sin ser detectado y tardó otros dos en ser reportado al público (Guiznar, 2017). Esquifa cometió aún más errores, el más notorio al liberar un sitio donde los consumidores podrían verificar si estaban o no afectados, y entregando información aparentementealeatoria, generandoaúnmás dudas sobresusistema de seguridad.

Este ataque es uno de los más notables entre decenas que se han reportado en el año, algunos de los cuales son:

• Un intento de extorsión a Bell Canadá que culminó

Con la filtración de los registros de 1.9 millones de clientes de la compañía (Sharp, 2017). • Ataques a dos grandes empresas en la industria de la hospitalidad, IHG (administradora de hoteles como Holiday Inn) (IHG, 2017) y Sabré (cuyo SynXis es

Usado por más de 32,000 hoteles) (Krebs, 2017). Aunque a primera vista esto se

Trata de un año más en la seguridad informática, lo interesante es la tendencia al "gran golpe" que los atacantes han perseguido. El ISTR de Symantec reporta, en su edición 2017, un promedio de 1314 incidentes de divulgación de información por año en el periodo de 2014-2016 (Symantec, 2017). El número de incidentes que involucran la divulgación de más de 10 millones de identidades va al alza, de 11 en 2014 a 13 en 2015, y a 15 en 2016.

10. Álvaro Gómez vélites. (2015). enciclopedia de la seguridad informática. México: alfa omega.

Objetivo

Abordar desde un punto de vista global la problemática de la Seguridad Informática

Y la Protección de Datos, contemplando tanto los aspectos técnicos, como los factores humanos y organizativos, así como el cumplimiento del entorno legal

En las propias empresas, la creciente complejidad de las relaciones con el entorno y el elevado número de transacciones realizadas como parte de su actividad han propiciado el soporte automatizado e informatizado de muchos de sus procesos, situación que se ha acelerado con la implantación de los ERP, o paquetes software de gestión integral. Por todo ello, en la actualidad las actividades cotidianas de las empresas y de las distintas Administraciones Públicas e, incluso, las de muchas otras instituciones y organismos, así como las de los propios ciudadanos, requieren

Del correcto funcionamiento de los sistemas y redes informáticas que las soportan y, en especial, de su seguridad. De ahí la gran importancia que se debería conceder

A todoslos aspectosrelacionados conla seguridad informáticaenuna organización.

La proliferación de los virus y códigos malignos y su rápida distribución a través de redes como Internet, así como los miles de ataques e incidentes de seguridad que

Se producen todos los años han contribuido a despertar un mayor interés por esta cuestión

11. Hugo Scolnik. (2011). Una mirada a la seguridad informática. Serie de conocimiento,12, 142.esitorial Trillas. México

Objetivo

Tratar de disminuir en la medida de lo más posible los ataques de usuarios internos y externos, virus informáticos, robo de información para lo cual se pueden

implementar medidas de seguridad monitoreo entorno al sistema de red con que cuenten dichas instituciones

Una mirada a la seguridad informática

Los hackers intentan penetrar tus dispositivos de muchas maneras distintas. Inclusive pueden usar la cámara de video para espiarte. La solución es tener instalado un cortafuego (denominado “firewall” en inglés).

Los hay muy buenos y gratuitos en la web. ENCRIPTACIÓN DE DATOS: Para proteger tu información sensible lo mejor es encriptar los datos y afortunadamente hay software recomendable y gratuito, tanto para proteger archivos como discos (por ej.: www.truecrypt.org).

ACCESO A SITIOSWEB: Los sitios seguros se identifican por un candadito de color

Amarillo.

Hay que clickear en ellos para comprobar que no sean sólo una imagen y verificar el certifica do digital que protege las transacciones con esos sitios. Cuando uno se conecta a un sitio Seguro, el certificado digital del mismo que contiene su clave pública se instala en nuestra

PC y permite que todo lo que hagamos se encripte usando dicha clave. De ese modo, Este proceso se lleva a cabo mediante un Protocolo especial llamado https (HyperText Transfer Protocol Secure). Es interesante

Observar que ninguna tarjeta de crédito ha reportado fraude en transacciones realizadas a través de sitios seguros pero, sin embargo, al usuario normal le parece que es más confiable entregar su tarjeta a un mozo de restaurant quien tendría la oportunidad de copiar sus datos o clonarla con dispositivos especiales. Hay proveedores a nivel mundial que ofrecen sitios con software de aplicación actualizado, controles de seguridad al nivel requerido y con mucho espacio físico para procesar toda la información que necesitemos. Para preservar nuestra privacidad se utilizan mecanismos de encriptación de datos.

12. Cibercriminología: Guía para la Investigación del Cibercrimen y Mejores Prácticas en Seguridad Digital

Objetivos Se busca instruir en la preservación de la evidencia digital en diferentes y complejos medios tecnológicos como principal factor en la optimización de la seguridad informática y la reducción de la impunidad

Las escuelas y universidades suelen ser lugares amigables donde las personas colaboran estrechamente en sus trabajos, por lo que para muchos es natural compartir nombres de usuario y contraseñas con colegas o dejar los equipos abiertos conectados a la red con su propio usuario. Lamentablemente, esta conducta puede perjudicar totalmente una de las mejores armas que tenemos para proteger los equipos: el análisis de registros.

Las copias de seguridad de los datos y los sistemas constituyen la última línea de defensa (y la mejor) ante los delincuentes destructivos. En el caso de una amenaza

Como el secuestro de información o ransomware, puede ser la única forma de ganarles a los malos. Quizás quieras considerar hacer la copia de seguridad en la nube, pero hazlo como un complemento y no como un reemplazo de las copias de seguridad locales, que se comprueban y almacenan en forma segura.

Cuandolos empleadosrotandeempleoylos alumnos dejanla institución, asegúrate de modificar sus credenciales consecuentemente. En muchos casos, esto significa cerrar sus accesos a los sistemas de la escuela. El uso de credenciales “persistentes” que tendrían que haberse suspendido es una de las formas más comunes del abuso “interno” de sistemas.

Y si los profesores, empleados y alumnos se van abruptamente y no quedan en buenos términos, es imprescindible cancelar todos sus accesos de inmediato.

Además, se debería hacer una verificación de las cuentas de usuario autorizadas al menos una vez al año para eliminar permisos que ya no son apropiados.

13. purificación aguilera López. (2015). seguridad informática. México: edites.

Objetivo

Determinar las acciones a realizar en una entidad durante el diseño, la implementación y posterior operación de un sistema de gestión de la seguridad informática

La realización del análisis y evaluación de los riesgos de seguridad y la selección de controles adecuados

En esta primera etapa se crean las condiciones para la realización del diseño, implementación y gestión de sistema de seguridad informática, para lo cual se realiza un estudio de la situación del sistema informático desde el punto de vista de

Seguridad, con el fin de determinar las acciones que se ejecutaran en función de las necesidades detectadas y con ello establecer las políticas, los objetivos, procesos y procedimientos de seguridad apropiados para gestionar el riesgo y mejorar la seguridad informática, posibilitando obtener resultados conforme con las políticas y objetivos globales de la organización

14. Gustavo Martínez ramos. (2015). seguridad informática. México: calameo.

Objetivo

Implementar sistemas de seguridad para la información que posee una organización y que puede ser vulnerada en cualquier momento, se recomiendan distintos niveles de protección a nivel software y hardware para protección y seguridad de toda una red organizacional

Aspectos sobre la seguridad de la información

La seguridad de la información se puede clasificar en tres aspectos importantes: Seguridad de las computadoras

Seguridad de la Red (Intranet)

Seguridad de Redes Interconectadas (Internet) No existe una frontera clara entre estos tres aspectos, debido a lo interrelacionados que están entre sí. La seguridad de las redes de computadoras se puede organizar en tres aspectos, a saber:

Existen diversos tipos de ataques que se pueden realizar a un sistema de comunicaciones, y dependiendo del tipo dependerá también la respuesta que se pueda plantear ante estos. En este apartado se ahondara un poco sobre este asunto.

Si los ataques se encuentran dirigidos directamente hacia los datos que se están comunicando pueden entrar dentro de las siguientes categorías:

Interrupción

Esto se refiere cuando se interrumpe totalmente el flujo normal de las comunicaciones, debido a que una parte o todo el sistema no pueden utilizarse. Ejemplo: destrucción física de equipos, borrada de aplicaciones, falla de sistema operativo, etc.

Intercepción

Esto se refiere a cuando hay algún acceso no autorizado al sistema, por parte de una persona, software o sistema de comunicación y debido a que no se pierden datos es uno de los ataques más difíciles de interceptar. Ejemplo: reproducción ilícita de archivos, intercepción de los cables para monitoreo de datos en una red, etc.

15 Gonzalo Álvarez Marañón. (2017). a mi lista de deseos seguridad informática para la empresa y particulares. México: McGraw- Hill.

Objetivo

Alcanzar un nivel de seguridad razonable, capaz de satisfacer las expectativas de seguridad de particulares y de pequeñas y medianas empresas

Fundamentos en la gestión de riesgos

Los fundamentos de la gestión del riesgo mediante la definición de objetivos de seguridad y la implantación de las medidas de seguridad más adecuadas para satisfacer las expectativas, mitigando los riesgos.

Protección del anonimato y de la privacidad en Internet.

Las medidas de seguridad a implantar para cumplir con las exigencias legales de la LOPD y la LSSICE.

Prevención y eliminación del spyware.

Protección de la confidencialidad de la información mediante el cifrado con EFS y SSL.

Protección de la disponibilidad de la información mediante sistemas tolerantes a fallos, estrategias de recuperación de sistemas y copias de seguridad, así como planes de contingencia.

Utilización de las firmas electrónicas y de los certificados digitales.

Cómo proteger redes Ethernet y redes inalámbricas frente a las amenazas más comunes.

Cómo elegir y utilizar los cortafuegos más adecuados a sus necesidades. Cómo crear y configurar una red privada virtual.

Fortalecimiento de los equipos de su red, su sistema operativo ,sus comunicaciones y sus aplicaciones, tanto en clientes como en servidores.

Cómo protegerse contra el malware: virus, gusanos, troyanos, contenido activo malicioso, etc.

Qué hacer para mantener a raya el spam, tanto en servidores de correo como en los equipos de los usuarios.

16 Jorge Ferrer, Javier Fernández-Sanguino. (2015). seguridad informática y software libre.. México: trillas.

Objetivo

Reconocer las ventajas ofrecidas por el software libre en el área de la seguridad informática, comparando éstas con las ofrecidas, hoy en día, por el software propietario.

Por qué son necesarios los mecanismos de seguridad?

Para poner de relevancia lo comentado en los párrafos anteriores se han elegido tres casos genéricos que se describen a continuación. Con ellos se pretende mostrar alguno de los peligros, relativos a seguridad, de estar 'interconectados'. Para cada uno de ellos existen mecanismos de seguridad que permiten llevar a cabo las operaciones de manera satisfactoria.

Cuando se intercambia información con un ordenador remoto, esa información circula por una serie de sistemas intermedios que son desconocidos a priori (excepto en ámbitos muy específicos). Además, no sólo no se sabe cuáles serán estos sistemas intermedios, sino que ademásno se dispone de ningún control sobre

Ellos o sobre lo que puedan hacer con nuestros datos al pasar por ellos. Quizá el propietario original es de fiar pero su sistema ha sido comprometido por un atacante

Que toma posesión de los datos enviados. Por otro lado tampoco se puede estar seguro de que el sistema al que uno se está conectando es quien dice ser. Existen diversos medios técnicos para suplantar la identidad de un sistema y engañar a un tercero cuando realiza la conexión. En definitiva, no existe una certeza absoluta de que aquellos sistemas a los que uno envíe información sean realmente los auténticos; además, en el caso de que lo sean no se sabe si les llegará la información que se les envía, o si llegará sin cambios o si, aún si llega sin modificaciones, será leída por terceras partes

17. Jorge Domínguez Chávez. (2015). Seguridad Informática Personal y Corporativa. México: IEASS, Editores.

Objetivos

Busca implantar un modelo de seguridad orientado al cumplimiento de normas, procedimientos y estándares informáticos con el objetivo de

Crear una cultura de seguridad en la organización, mejorando las seguridades

Existentes requeridas para la salvaguarda de la integridad de los recursos Informáticos.

Clasificar la información corporativa

Con la clasificación de la información se pueden priorizar y enfocar las acciones en materia de la gestión de la seguridad. La clasificación depende de la Naturaleza del negocio pero en general deberían incluirse tres niveles: información Pública, incluye todos los datos de dominio público. Ya que es información a la que Pueden acceder los clientes y proveedores, sus características

Principales deben ser la Precisión y la disponibilidad. En el siguiente nivel está la información de uso interno, Comprende toda la información que se intercambia al interior de la empresa y entre Los empleados, es la columna vertebral de las operaciones del negocio, por lo tanto las Características que le aplican son la disponibilidad y la integridad. En el último nivel Está la información de acceso restringido, está muy relacionada con el tipo de Actividad que puede incluir,

Por ejemplo los planes de negocio, información de nuevos productos, resultados de investigaciones o nuevas estrategias de mercado. La principal característica de este tipo de información es su confidencialidad.

Al clasificar la información, la empresa tiene un panorama más claro de cuáles son los aspectos en los que debe enfocar sugestión. De esta forma se pueden identificar

Cuáles son los riesgos más relevantes dentro del SGSI y por tanto, determinar los controles más apropiados y acordes a la realidad de la empresa

18. Silvia M. Quiroz-Zambrano, David G. Macías-Valencia. (2017). Seguridad en informática: consideraciones. México: Alfaro.

Objetivo

El objetivo primario de la seguridad informática es el de mantener al mínimo los riesgos sobre los recursos informáticos, -todos los recursos- y garantizar así la continuidad de las operaciones de la organización al tiempo que se administra ese

Riesgo informático a un cierto costo aceptable. Para ello utilizaremos estructuras organizacionales técnicas, administrativas, gerenciales o legales.

Vulnerabilidades informáticas

Amenazas informática. Los primeros virus informáticos surgieron como experimentos en universidades, juegos, o simplemente con el propósito de molestar, pero no directamente con el objetivo de causar daños en los equipos informáticos

Así los primeros virus datan de los años 70, cuando el uso de ordenadores no era popular Por otro lado ya no tienen sólo como objetivo dañar el sistema, si no que pueden sustraer información sensible del equipo informático (contraseñas, números

De tarjetas de crédito, etc...) O utilizar el equipo para realizar ataques a otros sistemas a través de él Los pasos a seguir para mejorar la seguridad son los siguientes: Identificar los activos, es decir, los elementos que la empresa quiere

Proteger. Formación de los trabajadores de las empresas en cuanto a materias de seguridad. Concienciación de la importancia de la seguridad informática para los trabajadores de la empresa. Evaluar los riesgos, considerando el impacto que pueden tener los daños que se produzcan sobre los activos y las vulnerabilidades del sistema. Diseñar el plan de actuación, que debe incluir:

19. Daniel Felipe González Agudelo. (2014). el riesgo y la falta de políticas de seguridad informática una amenaza en las empresas certificadas. México: Edomex.

Objetivo

Estándares de seguridad de la norma BASC, el cual menciona la seguridad en las tecnologías de la información (protección con contraseñas, responsabilidad y protección a los sistemas y datos). El tema a desarrollar se enfoca en la problemática que conlleva no tener políticas, procedimientos y/o normas de

seguridad informática en las empresas certificadas BASC. La protección de datos, documentos y control de acceso a la información es un tema que cada día toma más fuerza en las grandes compañías, debido a las diferentes especialidades de hackers y crackers que roban información vital

Definir una política de seguridad

Definir una política de seguridad de red significa elaborar procedimientos y planes que salvaguarden los recursos de la red contra pedida ydaños. Unode los enfoques posible para elaborar dicha política propondrá examinar lo siguiente:

- Que recursos está usted tratando de proteger
- De quienes necesita proteger los recursos
- Que tan posibles son las amenazas.
- Que tan importante es el recurso

- Qué medidas puede implementar para proteger sus bienes de forma económica y oportuna

Examinar periódicamente su política de seguridad de red para ver si han cambiado

Los objetivos y las circunstancias de la red. En general el costo de proteger las redes de una amenaza debe ser menor que el de recuperación en caso de que se viera afectado por una amenaza de seguridad si no se tiene el conocimiento suficiente de lo que se está protegiendo y de las fuentes de amenaza, puede ser difícil alcanzar un nivel aceptable de seguridad. Es importante hacer que en el

diseño de la política de seguridad participe la gente adecuada. Un aspecto importante de la política de seguridad es asegurar que todos conozcan su propia responsabilidad para mantenerla, es entendible que este conjunto de normas llamadas políticas se anticipen a todas la amenazas que existen, sin embargo, esta no puede asegurar que para cada tipo de proceso haya alguien que lo pueda manejar de manera consciente y responsable.

20. Sergio Andrés Becerril. (2017). confidencialidad de la información. 31, 5, 114

Objetivo

Los efectos y algunas reflexiones a raíz del ataque de WannaCry. Se aborda cómo funciona la red Torrent y por qué puede ser una alternativa para proteger la seguridad durante la navegación en Internet. También se hace un recuento del ransomware desde sus inicios hasta la fecha.

Además se habla sobre los riesgos y ventajas de los servicios que usan una sola contraseña para acceder a diferentes servicios. Se explica por qué los torrents son una amenaza a la seguridad a pesar de ser una forma legítima de intercambio de información. Finalmente, se muestra cómo usar Thug, un cliente del proyecto honeypot que simula un navegador y colecta los resultados de su actividad para estudiar, analizar y localizar paquetes de exploits y sitios web maliciosos.

La utilización del internet y correo electrónico prevención para posibles ataques

En estos últimos años se han incrementado de forma significativa los conflictos legales sobre la utilización de Internet y del correo electrónico y, a falta de una clara normativa, se han dictado sentencias a favor de unos y otros, empresarios y trabajadores, avalando en unos casos despidos por abuso de Internet y rechazándolos en otros. Por todo ello, la implantación de un Sistema de Gestión de Seguridad de la Información debería contem-plar el factor humano como uno

De sus elementos clave, contemplando aspectos como la adecuada formación y sensibilización de los empleados, la implicación de los responsables y directivos, la aprobación de un Reglamento Interno sobre el uso de la Informática e Internet en la organización, etc., cuestiones que se analizarán con detalle en este trabajo.

La implantación de unas adecuadas medidas de seguridad informática exige contemplar aspectos técnicos (antivirus, cortafuegos, IDS...), organizativos (planes y procedimientos) y legales (cumplimiento de la legislación vigentes sobre protección de datos, uso de la firma electrónica, propiedad intelectual, etc.). No obstante, en muchas ocasiones se presta muy poca atención a la importancia del factor humano en la seguridad informática. Además, hay que tener en cuenta que una empresa u organización puede ser responsable subsidiara por los actos de sus empleados

21. Francisco Montesinos. (2018). Seguridad Informática: Un tema de responsabilidad gerencial. El economista, 30, 12

Objetivo

Construir un plan pues allí se define claramente el rumbo y los objetivos de seguridad de la información, de forma que estén alineados a los objetivos de negocio; tarea vital para la adecuada gestión de riesgos. Sin embargo, la estrategia

de seguridad no debe ser compleja, sino simple, pero robusta y que abarque todas las necesidades particulares de la empresa Alcance del Plan de Seguridad informática El alcance expresará el radio de acción que abarca el Plan, de acuerdo al Sistema Informático objeto de protección, para el cual fueron determinados los riesgos y diseñado el Sistema de Seguridad. La importancia de dejar definido claramente el alcance del Plan (y de ahí su inclusión al comienzo del mismo) consiste en que permite tener a priori una idea precisa de la extensión y los límites

en que el mismo tiene vigencia. Las políticas que se describan comprenden toda la

Organización, ya que es obligatorio su cumplimiento en las áreas que las requieran, razón por la cual serán lo suficientemente generales y flexibles para poder implementarse en cada caso mediante las medidas y procedimientos que demanden las características específicas de cada lugar.

22. SUSANA MENDIETA. (2017).Gobierno de la CdMx busca mejorar ciberseguridad. milenio, 35

Objetivo

Evitar el robo de identidad a través del phishing obtener datos personales de los usuarios de Internet con sitios falsos, acceso a una computadora a la distancia y sin el consentimiento del propietario

Sistemas de protección

Los sectores que han desarrollado con éxito sistemas de protección son el financiero, bancario y el energético; sin embargo, incluso los más preparados para evitar un ciberataque suelen no poder blindarse completamente Los Estados nacionales han sido poco eficaces para crear marcos jurídicos para desarrollar políticas públicas que ayuden a reducir la sobrexposición al riesgo de sus ciudadanos y menores de edad. Muchos han errado en el intento para lograr una legislación exitosa que al mismo tiempo sea eficiente y respete la privacidad y la libertad de expresión de los usuarios de la red. La ciberseguridad se define según la Unión Internacional de Telecomunicaciones como el conjunto de herramientas, políticas, conceptos, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Otra definición de ciberseguridad es aquellas actividades orientadas

A responder a determinadas amenazas que, usando la tecnología y el internet como medios, puedan verse amplificadas Los expertos señalan que una estrategia nacional para la ciberseguridad debe incluir la existencia de un órgano de coordinación al más alto nivel gubernamental para supervisar, coordinar y ajustar lo necesario. Incluir al sector privado es fundamental para la cooperación ante situaciones delicadas

23 .Maíllo Fernández, Juan Andrés. (2017). Seguridad Digital e Informática. México: Rama

Objetivos

Cumplir los objetivos empresariales de manera organizada, segura y transparente para los directivos asegurando que la pérdida de información, los ataques dirigidos y el robo de identidades no ocupen la mente de las personas que generan el negocio.

¿Qué es la Seguridad digital?

La seguridad informática, también conocida como ciberseguridad o seguridad de tecnologías de la información, es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta, especialmente la información contenida o circulante. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información.

La seguridad informática comprende software (bases de datos, metadatos, archivos), hardware y todo lo que la organización valore y signifique un riesgo. Si esta información confidencial llega a manos de otras personas, se convierte automáticamente en un riesgo para toda la organización

24 Lourdes López, Eloy Portillo. (2010). Seguridad en redes telemáticas Parte I: La problemática de la seguridad. México: paraninfo

Objetivo

Brindar los conocimientos amplios y de actualidad sobre los elementos más relevantes en ciberseguridad para reconocer las principales amenazas cibernéticas, permitiéndoles así iniciar o mejorar la cultura de ciberseguridad en su organización

El analista y experto en seguridad “Kaspersky Lab” en su boletín de seguridad «Estadísticas Generales de 2016» menciona que:

El 31.9% de los equipos de los usuarios sufrieron al menos un tipo de ataque con programas maliciosos desde Internet en dicho año

A nivel global se registraron 262 millones de URLs maliciosos y 578 millones de ataques On Line en todo el mundo, de los cuales 29% se originaron en EEUU

Entre los ataquesmás relevantes duranteel 2016semencionael “DDoS” queafectó a empresas como Netflix, Spotify y empresas bancarias como el de Saguaro y el ataque a servidores de Yahoo, afectando no sólo a las organizaciones si no a millones de usuarios

México es el segundo país más atacado en América Latina y a nivel mundial ocupa la posición 8, lo que se debe a la falta de conciencia de usuarios sobre su vida y lo digital, así como la falta de prácticas de seguridad efectivas en las organizaciones

Ante tal escenario, se vuelve necesario contar con el conocimiento suficiente para entender las principales amenazas y vectores de ataques cibernéticos.

25 Juan Voutssas M.*. (2010). Preservación documental digital y seguridad informática. investigación bibliotecológica, 24, 125.

Objetivo

Se analiza la problemática actual de la producción y acumulación mundial de información en forma de documentos electrónicos o digitales, así como los problemas derivados del acceso de esa información, sobre todo en red, dado que esto podría implicar riesgo y pérdida de esa información. Se determinan los riesgos, amenazas vulnerabilidades, etcétera, que afectan a esa información, así como diversas estrategias para establecer la seguridad informática y la relación de ésta con la preservación confiable de esa información. Se estudian y establecen con detalle los factores que inciden a favor y en contra de los documentos digitales

El ambiente de los sistemas de información.

En la actualidad, los sistemas de información han sido sustituidos casi en su totalidadporTecnologías deInformaciónyComunicaciones (TIC) convergentes, por inmensas y cada vez más complejas redes institucionales locales y regionales, por servidores y computadoras personales que cada vez tienen mayor capacidad de proceso y de acceso a otros computadores, y cuya interconexión se extiende mundialmente. Al mismo tiempo, la Internet forma ya parte de la infraestructura operativa de sectores estratégicos de todos los países como el comercial, energía,

transportes, banca y finanzas, -por mencionar algunos- y desempeña un papel fundamental en la forma en que los gobiernos proporcionan sus servicios e interactúan con organizaciones, empresas y ciudadanía, y es un factor cada vez más creciente de intercambio de información de manera individual por parte de los ciudadanos toda vez que se forman redes sociales cada vez más complejas conceptos fundamentales de la seguridad informática:

Para poder comprender el concepto integral de la seguridad informática, es indispensable entender los diversos conceptos básicos que la rigen, ya que de otra forma no es posible establecer una base de estudio. Los enunciaré a continuación y los desarrollaré con más detalle más adelante.

- Recursos Informáticos: el equipo de cómputo y telecomunicaciones; los sistemas, programas y aplicaciones, así como los datos e información de una organización. También se les conoce como "activos informáticos"

- Amenaza: fuente o causa potencial de eventos o incidentes no deseados que pueden resultar en daño a los recursos informáticos de la organización.

- Impacto: la medida del efecto nocivo de un evento.

- Vulnerabilidad: característica o circunstancia de debilidad de un recurso informático la cual es susceptible de ser explotada por una amenaza.

- Riesgo: la probabilidad de que un evento nocivo ocurra combinado con su impacto en la organización.

- Principio básico de la seguridad informática: la seguridad informática no es un producto, es un proceso.

AMENAZAS INFORMÁTICAS

Las amenazas, como ya hemos mencionado, consisten en la fuente o causa potencial de eventos o incidentes no deseados que pueden resultar en daño a los

insumos informáticos de la organización y ulteriormente a ella misma. Entre ellas, identificamos como las principales:

•El advenimiento y proliferación de "malware" o "malicioso software", programas cuyo objetivo es el de infiltrase en los sistemas sin conocimiento de su dueño, con objeto de causar daño o perjuicio al comportamiento del sistema y por tanto de la organización.

- La pérdida, destrucción, alteración, o sustracción de información por parte de personal de la organización debido a negligencia, dolo, mala capacitación, falta de responsabilidad laboral, mal uso, ignorancia, apagado o elusión de dispositivos de seguridad y/o buenas prácticas.

- La pérdida, destrucción, alteración, sustracción, consulta y divulgación de información por

- El acceso no autorizado a conjuntos de información.

- La pérdida, destrucción o sustracción de información debida a vandalismo.

- Los ataques de negación de servicio o de intrusión a los sistemas de la organización por parte de cibercriminales: personas o grupos malintencionados quienes apoyan o realizan actividades criminales y que usan estos ataques o amenazan con usarlos, como medios de presión o extorsión.

- Los "phishers", especializados en robo de identidades personales y otros ataques

del tipo de "ingeniería social"

- Los "spammers" y otros mercadotecnitas irresponsables y egoístas quienes saturan y desperdician el ancho de banda de las organizaciones.

- La pérdida o destrucción de información debida a accidentes y fallas del equipo: fallas de energía, fallas debidas a calentamiento, aterrizamiento, des

magnetización, ralladura o descompostura de dispositivos de almacenamiento, etcétera.

- La pérdida o destrucción de información debida a catástrofes naturales: inundaciones, tormentas, incendios, sismos, etcétera.

- El advenimiento de tecnologías avanzadas tales como el cómputo quantum, mismas que pueden ser utilizadas para desencriptar documentos, llaves, etcétera al combinar complejos principios físicos, matemáticos y computacionales

26. Paul Lara. (2016). Paul Lara. Maxis, 20, 117. Objetivo

Invertir en un sistema de seguridad, sobre todo de un proveedor externo que se dedique a tener la tecnología de vanguardia y actualizada día a día, puede parecer una propuesta costosa, pero las pérdidas de un ataque exitoso pueden conllevar a la pérdida de todo el patrimonio.

Para muchas empresas, todo parece demasiado fácil cuando se trata de la necesidad de seguridad en TI, pues simplemente no se preocupan en invertir. Su alegato: no creen ser considerados víctimas de un ataque cibernético o no han tenido alguna falla que los lleve a perder horas fuera de línea, con su respectiva pérdida en ingresos. Se dicen “blindados”.

Sin embargo, la sorpresa que se llevan muchos especialistas cuando preguntan a directivos de los corporativos cuál es el nivel de protección tiene que ver con una respuesta común: un software antivirus.

Desde hace ya varios años, las violaciones y robos de datos a menudo se leen en los titulares de los diarios y las noticias, como fue el caso de Home Depot y Target hace algunos meses.

Las historias tienden a ser dadas a conocer cuando se trata de corporativos muy conocidos, por grandes pérdidas millonarias, millones de datos de usuarios o trabajadores o información financiera. Sin embargo, hoy nadie está exento del

Cibercrimen, y creer que se tiene la seguridad total de la TI con poca inversión, es un riesgo.

Miles de empresas sufren violaciones de datos, y aunque creen que no están perdiendo dinero, puede que si al no darse cuenta de la fuga de secretos industriales, robo de identidad o información clave para cerrar un negocio.

Necesidad de seguridad: el momento crítico

Según la compañía de ciberseguridad Symantec, desde 2013 hay un aumento en la proliferación de violaciones a la seguridad de las empresas y gobiernos con fines

Financieros.

“Los hackers se infiltraron en decenas de empresas y gobiernos, incluidas muchas instituciones de América Latina y el Caribe, para lograr acceso a información confidencial. Se produjeron 253 violaciones de datos a gran escala en 2013, lo que representó un aumento de 62% respecto de 2012.05 Ocho de estas violaciones de datos expusieron diez millones de identidades o más cada una, lo cual obligó a comerciantes minoristas, empresas financieras, de seguros y personas físicas, a invertir una gran cantidad de tiempo y recursos financieros para responder y recuperarse de esos ataques e implementar mecanismos de protección adicionales”, se asegura en el análisis.

La mayoría de los ataques hoy se relacionan con virus, gusanos, troyanos y malware. Este tipo de violaciones cuestan mucho dinero.

7. IDENTIFICAR LOS ACTIVOS SENSIBLES

7.1 IDENTIFICACIÓN Y VALORIZACIÓN DE ACTIVOS

Comenzaremos explicando a que se le llama activo sensible en informática para ir teniendo una idea más clara durante el desarrollo de esta tesis.

Se le llama activos sensibles de información a aquellos recursos de software y hardware con los que toda empresa, organización o institución cuenta y con la que compone un sistema de comunicación partiendo desde la información, el emisor el medio de transmisión y receptor.

A continuación, se mencionan algunos ejemplos de los activos para lograr una mejor comprensión en la identificación de estos:

-servidores

-routers

-racks

-cables de red

-swicht

-aplicaciones

-sistemas operativos

-programas computacionales

-bases de datos

Estos son solo algunos ejemplos de activos sensibles de información, existe una metodología para agruparlos llamada Magerit que más adelante se describirá en que consiste y como se utiliza, y en base a esta se realiza una identificación de activos pudiendoenlistar a estos de unamanera clara yordenada. Aesto se le llama análisis de riesgos informáticos

Para identificar y proteger los activos sensibles que existen en una empresa o institución para fines de una implementación de políticas de seguridad es necesario elaborar un inventario que los identifique y clasifique, cada activo en el inventario deberá incluir al menos su descripción, localización y propietario.

Una vez identificados todos los activos hay que realizar un análisis de la dependencia existente entre ellos.

Se puede decir simplemente que un activo depende de otro o también se puede clasificar por el grado de dependencia, esto es, el grado de porcentaje de cuanto se vería P afectado como consecuencia de la destrucción de H.

Valoración de activos

No todos los activos de una organización son de la misma importancia unos son más importantes que otros y por consiguiente los problemas que puedan surgir de un ataque son distintos y es por esta razón que se debe realizar una valorización de los activos en función de la relevancia que tengan para la institución y obviamente el impacto que pueda tener o causar a la organización

Valorización cuantitativa

Se estima el valor económico del activo

Valorización cualitativa

Esta seestablece deacuerdoa unaescala´por ejemplo del 0al 10,o bajo,medió, alto y el criterio que generalmente se aplica es basado en las características principales de la información, integridad, confidencialidad e integridad.

Por ejemplo, si se considera a una base de datos como activo de la organización su valorización tiene que hacer de acuerdo estas tres últimas características principales

7.2 CLASIFICACIÓN DE ACTIVOS EN EL INVENTARIO

La información que se plasma en un inventario de activos puede variar dependiendo del alcance del mismo. Se recomienda que exista un equipo de seguridad que se encargue de gestionar y actualizar, así como su revisión anual tras cada incorporación o eliminación de activos, este equipo será responsable de tareas como la definición, el inventariado y la categorización de los diferentes activos dentro de los sistemas de control, así mismo las redes internas y externas según el alcance del inventario

La identificación del inventario de activos de información, permite clasificar los activos a los que se les debe brindar mayor protección, pues identifica claramente sus características y rol al interior de un proceso.

El análisis de riesgos informáticos es un proceso que comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos, así como su probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo.

Las actividades a realizar para obtener un inventario de activos son:

Definición, Revisión, Actualización y Publicación.

Definición. Se determina que activos sensibles van a hacer parte del inventario esto supervisado por un grupo y líder de proyecto al interior de la organización se recomienda que la definición se realice cada año

La información básica que debe llevar la definición es la siguiente:

- -identificador: número que identifica al activo
- -proceso: nombre del proceso al que pertenece el activo
- -nombre activo Nombre de identificación del activo dentro del proceso al que pertenece.
- Descripción/Observaciones: espacio para describir el activo para que lo identifique cualquier miembro del proceso

- Tipo: tipo al cual pertenece el activo. Para este campo como puede ser bases y archivos de datos, contratos, documentación del sistema, investigaciones, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planespara la continuidadde lainstitución,acuerdos sobre retiro y pruebas de auditoría, entre varios más.
- Software: De aplicación, de interfaces, software de sistema, herramientas de desarrollo y otras utilidades.
- Recurso humano: Son todas las personas que, por su conocimiento y experiencia para el proceso, se les considera activos de información.
- Servicio: Internet, páginas de consulta, directorios compartidos e Intranet. Hardware, Equipos de cómputo y de comunicaciones que por su criticidad son considerados activos de información, no sólo activos fijos.
- Ubicación: Se refiere a la ubicación física como electrónica del activo de información.
- Clasificación: Se refiere a la protección de información de acuerdo a Confidencialidad, Integridad y Disponibilidad.

- Justificación: Para cada valoración, describe el impacto que causaría la pérdida de la propiedad (Confidencialidad, Integridad y Disponibilidad), o el argumento del porque se asignó dicha valoración.
- Criticidad: Es un cálculo automático que determina el valor general del activo, de acuerdo con la clasificación de la Información:

- Alta. Activos de información en los cuales la clasificación de la información en todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
- Media. Activos de información en los cuales la clasificación de la información es alta en una de sus propiedades (confidencialidad, integridad, y disponibilidad) o al menos una de ellas es de nivel medio.
- Baja. Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.
- Propiedad o Propietario: parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con el proceso se clasifican adecuadamente. Se deben revisar frecuentemente las restricciones y clasificaciones del acceso.

- Custodio: hace referencia a un cargo, proceso, o grupo de trabajo encargado de supervisar las restricciones y clasificaciones de acceso definidos por el propietario. (Para sistemas de información o información consignada o respaldada, generalmente es TI o para información física, los custodios pueden ser los directivos o el proceso de archivo o correspondencia, el custodio generalmente se define donde se encuentra el activo original.
- Acceso Usuarios: Son quienes generan, obtienen, transforman, conservan, eliminan o utilizan la información, en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información.

- Gestión: Fecha ingreso del Activo: Fecha de ingreso del activo de información en el inventario
- Fecha salida del Activo: Fecha de exclusión del activo de información del inventario

Revisión

Se realiza para verificar si un activo sigue siendo o no parte del inventario, o si la evaluación o clasificación del activo debe ser en algún momento modificada

En general, el inventario de activos puede ser revisado o validado en cualquier momento previa autorización del líder del proceso o el oficial de seguridad de la información

Las razones por las cuales se puede realizar una revisión o validación son:

Actualizaciones al proceso al que pertenece el activo.

Adición de actividades al proceso

Inclusión de nuevos registros de calidad, nuevos registros de referencia o procesos y procedimientos.

Inclusión de un nuevo activo.

Desaparición de un área, proceso o cargo en la entidad que tenía asignado el rol de propietario o custodio (Cambios Organizacionales).

Cambios o migraciones de sistemas de información en donde se almacenan o

reposan activos de la ubicación ya inventariados.

Cambios físicos de la ubicación de activos de información.

Actualización Unavezse hadefinido quécambios serealizarían enel inventario, desde cada proceso, se procede a actualizar el inventario de activos de información.

Publicación El inventario de activos de información debe ser un documento clasificado como “Confidencial”, y no debe tener características que se permitan modificar por los usuarios autorizados. Sólo debe tener acceso de modificación a este documento el líder del proceso con previa autorización del oficial de seguridad de la información.

7.3 INVENTARIO Y CLASIFICACIÓN DE LOS ACTIVOS SENSIBLES DEL DEPARTAMENTO DE SERVICIOS EDUCATIVOS

Realización del inventario.

En este procedimiento el objetivo es establecer la importancia y nivel de sensibilidad de los activos de información permitiendo conocer su valor para el departamento de servicios.

Para la realización del inventario deberemos tomar en cuenta lo siguientes parámetros:

Cada custodio de la información será responsable por la elaboración y actualización del inventario de activos de información.

El dueño del proceso se encargará de validar el inventario de archivos de información y solicitar las correcciones que pudiera existir

El proceso de inventario y clasificación de la información es de obligatoria ejecución y debe ejecutarse de forma inmediata y permanente en la medida que

nueva información para el departamento sea generada, exista un cambio en los procesos vigentes o exista un cambio en su importancia de riesgo.

La metodología de Magerit v3 de Análisis y Gestión de Riesgos de los Sistemas de Información permite agrupar a los activos para una mejor identificación y realizar de una manera más organizada el inventario de activos sensibles esta agrupación es la siguiente:

Tipo de activo

- De servicios.: procesos de negocio de la organización
- Datos de información: suele ser el núcleo del sistema
- Aplicaciones de software: programas computacionales
- Equipos informáticos: pc, laptop, impresoras, escáner, servidores
- Personal: personal interno. Subcontratados clientes
- Redes de comunicaciones: dan soporte a la organización para el movimiento de la información pueden ser redes propias o subcontratadas
- Soporte de información: son soportes físicos que permiten el almacenamiento de la información durante un largo periodo.
- Equipamiento auxiliar: dan soporte a los sistemas de información y son activos que no se han incluido en ninguno de los otros grupos
- Instalaciones: es el edificio o lugar donde se almacenan los activos de información

Recordemos que el criterio que se utilizara para la valoración y elaboración del inventario está basado en las características principales de la información: integridad, confidencialidad y disponibilidad.

Guía de inventario

1. Objetivo de la guía de inventarios: establecer los criterios, procedimientos y recomendaciones que se deben tomar en cuenta por los custodios de la información

2. inventario de activos de información: la definición de un inventario permite conocer cuáles son los activos de información más importantes de los procesos de la organización.

3.0. procedimiento de inventario: el procedimiento a ejecutar debe contener las actividades expuestas en la figura 1.

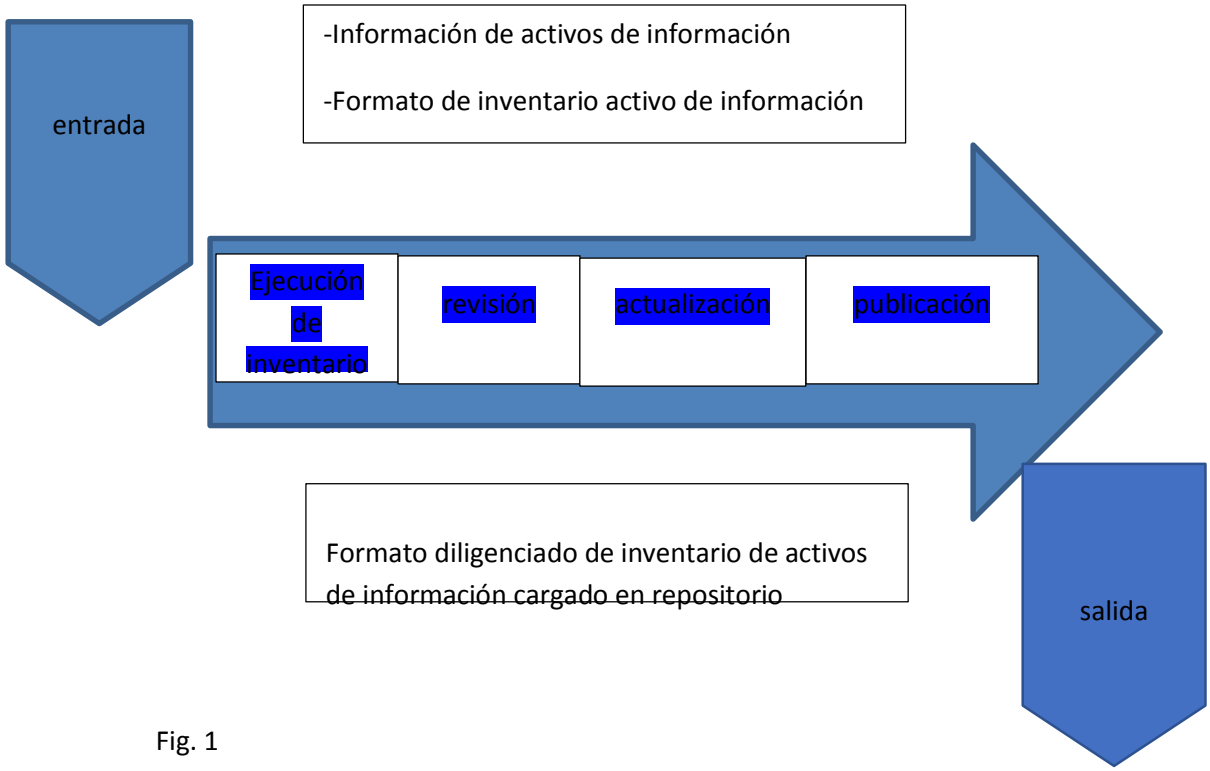


Fig. 1

4. realización del inventario

Se establece la importancia y el nivel de sensibilidad de los activos de información permitiendo reconocer su valor para el negocio

5. tipo de activo
Se define a que tipo pertenece el activo

*De servicios.
*Aplicacionesde software
Equipos informáticos
Personal
Redes de comunicaciones
Soporte de información
Equipamiento auxiliar
Instalaciones

6. propietario del activo. Es el responsable de los activos

7. custodios de la información. Responsables de proteger la información en su poder de acceso, alteración o destrucción no autorizada y de mantener la integridad y disponibilidad de la información a través del uso de controles de accesos apropiados

8. usuarios de la información. Son las personas a quienes el propietario de la información les ha dado la autorización, para acceder, modificar, borrar y utilizar información en el desempeño de su función laboral.

Inventario de activos de información sensibles.

Actualmente el departamento de servicios educativos tiene los siguientes activos de información e infraestructura tecnológica:

- Servidores y Equipos de Intercambio de Datos
- El departamento cuenta con 4 servidores.
- Encargado del control de acceso en el salón de sistema.
- Sistema Operativo Windows Server 2008, marca hp.
- Dos (2) zonas de acceso inalámbrico.
- Red de internet.
- Un swicht de red.
- 1 routers.
- 1 swicht
- Sistemas de Seguridad, Prevención y Control de Acceso
- Sensores de movimiento y alarmas de seguridad.
- Administrada por la misma institución.
- Cámaras de seguridad IP.
- Administrada por la misma institución.
- Sistema de aire acondicionado.
- Extintores de diferentes tipos según la ubicación del extintor, entorno, equipos y elementos de cada sitio.
- Equipos de Cómputo
- El departamentodisponede 13equipos decómputo, para usoadministrativo y docente.
- 2 impresoras
- 1 escáner
- 1 copiador

Tabla 1. Activos TIPO	NOMBRE DEL ACTIVO
APLICACIONES INFORMÁTICAS	1. [SI_SIGES] Sistema de Información Académica y de Gestión. 2. [SI_BD] SIMAT Sistema Integrado de Matriculas. 3. [SO] Sistema Operativo. 4. [HER_SW] Herramientas Software. 5. [ANT_VIR] Anti virus
SERVICIOS	6. [SV_DNS] Servidor DNS 7. [SV_DHCP] Servidor DHCP 8. [SV_VoIP] Servidor Telefonía IP 9. [SV_CAM] Servidor Cámaras IP
REDES DE COMUNICACIONES	10. [RO_ISP] Router Proveedor de Servicios de Internet.
EQUIPAMIENTO INFORMÁTICO	11. [FW_UTM] Firewall / Equipo Unificado contra Amenazas. 12. [PC] Equipos de computo 13. [SW_A] Swicht Administrable
EQUIPAMIENTO AUXILIAR	14. [CAB_RED] Cableado de Red
PERSONAL	15.[AS_TIC] Asesor Tecnologías de

	Información y Comunicaciones y control escolar 16.[TEC_ADMIN_II]Técnico Administrativo Grado II
INSTALACIONES	17. [GAB] Gabinete de red

8. LISTAR LAS PRINCIPALES AMENAZAS A LOS ACTIVOS CRÍTICOS DEL DEPARTAMENTO DE SERVICIOS EDUCATIVOS

.

8.1. MAGERIT UNA METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGOS PARA LISTAR AMENAZAS Y VULNERABILIDAD POR CADA TIPO DE ACTIVO.

La metodología MAGERIT v.3 para el análisis y gestión de las posibles fallas, amenazas y vulnerabilidades que se puedan estar presentando en el departamento de servicios afecta de forma directa o indirecta la seguridad de la información que se administra o manipula el personal administrativo y docente.

El objetivo de este proyecto es hacer énfasis en los servicios que actualmente se prestan en el departamento de la institución, siendo estos fundamentales en el funcionamiento diario donde se pueden presentar fallas, daños o alteraciones a dichos servicios por la ausencia de procedimientos, políticas, planes y mecanismos que garanticen la confiabilidad, confidencialidad y disponibilidad de la información

Evaluación de Vulnerabilidades

Cuadro 1: Evaluación de vulnerabilidades Evaluación de vulnerabilidades 1	
Prueba efectuada	, Dicha prueba se realizó utilizando Herramientas como Nmpa, ping y zenmap.
Fecha de duración	Febrero 5 – 7.00 am a 10.00 am (Direcciones públicas) Febrero 10– 7.00 a 10.00 (Direcciones privadas)
Encargado de prueba	Ing. Díaz
Conclusiones	Se pudo establecer que la protección de los firewalls se encuentra bastante restrictiva a nivel del direccionamiento público obedeciendo a las políticas establecidas de restricción de servicios y protocolos en el Firewall. En el direccionamiento privado se Detectaron puertos abiertos, debido a que no se han establecido políticas restrictivas, ya que se obtuvo

	Información de los servicios y puertos Abiertos.
Evaluación de vulnerabilidades 2	
Prueba efectuada	Una vez identificados los puertos y servicios específicos de los activos de la institución, se procede a ejecutar pruebas con herramientas que permitieron encontrar y analizar las vulnerabilidades, entre estas tenemos: Nessus y Nikto. Identificando fallos a nivel de sistemas operativos, aplicativos o servicios.

Evaluación de vulnerabilidades (Continuación) Activo de información	Servidores de sitios web críticos, por direcciones públicas, Sistemas de Servidores de Información logística (GLPI), Servidores SIMAT y Servidor SIGES.
Fecha de duración	Febrero 10 de 2023 (7.00 am,) hasta Febrero 14 de 2023 (10.00 am)
Encargado de prueba	
Conclusiones	De acuerdo a los resultados obtenidos provistos por las herramientas de detección de vulnerabilidades, se

	Establecieron vulnerabilidades tipo ransomware, como también en niveles de versiones obsoletas en sistemas operativos al igual que las versiones que tienen alto riesgo de amenazas y vulneración en servidores web.
Evaluación de vulnerabilidades 3	
Prueba efectuada	Se efectuaron pruebas al SIGES, determinando el desarrollo de módulos web, a nivel de scripts, variables y chequeo de código de bajo rendimiento.
Activo de información	Sistema de Información para la Gestión Escolar SIGES, se reconocieron los módulos internos y externos, determinando la evaluación en línea, generación de boletines y libros de notas de años anteriores.
Fecha de duración	Febrero 20 al 21 7 a 10 horas am
Encargado de prueba	Ing. Díaz
Conclusiones	Se pudo establecer que dentro de una prueba interna el rendimiento de algunos módulos se ven saturados frente a un script provocando denegaciones de un servicio después de un corto periodo de tiempo

Evaluación de vulnerabilidades (continuación) Evaluación de vulnerabilidades 4	
Prueba efectuada	Se efectuaron pruebas al SIMAT, determinando el desarrollo de módulos web, a nivel de scripts, variables y chequeo de código de bajo rendimiento.
Activo de información	Sistema Integrado de Matriculas SIMAT, se reconocieron los módulos internos y externos, determinando los alumnos matriculados en cada sede, la matrícula de un estudiante y el retiro de éste.
Fecha de duración	Febrero 27 y 28 7 a 10 am
Encargado de prueba	Ing. Díaz
Conclusiones	Se pudo establecer que dentro de una Prueba interna el rendimiento de algunos módulos se ven saturados frente a un script provocando denegaciones de un servicio después de un corto periodo de tiempo

Evaluación de vulnerabilidades 5

Prueba efectuada	Se realizaron pruebas de verificación de contraseñas a los sistemas web de acceso a SIGES y SIMAT.
Activo de información	Servidores web de SIGES y SIMAR.
Fecha de duración	Febrero 27 a 10 hrs
Encargado de prueba	Ing. Díaz
Conclusiones	Con la utilización de la herramienta de John The Ripper, se pudo establecer que las contraseñas no son seguras y que muchas son fáciles de descifrar en los sistemas web SIGES y SIMAT

Evaluación de vulnerabilidades (continuación) Evaluación de vulnerabilidades 6

Prueba efectuada De acuerdo a las vulnerabilidades

Activo de información	presentadas, se realizaron pruebas de penetración, utilizando las herramientas detipo httpprint comparandolas firmasde versionesdel web server objeto de análisis con las listas de explotación y fallas a nivel de configuración o codificación. Se realizará pruebas de vulnerabilidades a los servidores y aplicativos webs de SIGES y SIMAT que enlacen a los módulos o sistemas de información sensibles, los cuales fueron virtual izados por Virtual Box como ambiente de laboratorio de pruebas.
Fecha de duración	Marzo 5 de 7 a 10 am
Encargado de prueba	ING. DIAZ

Conclusiones	Se demostró que existen fallas de seguridad, como fueron las malas prácticas para la asignación de passwords.

8.2 ANÁLISIS DE RIESGOS AL DETALLE CON LA HERRAMIENTA PILAR

La herramienta PILAR estandarizada por MAGERIT v3; clasifica las amenazas en Cuatro grupos:

[N] Desastres naturales.

[I] De origen natural.

[E] Errores y fallos no intencionados.

[A] Ataque intencionado.

El objetivo es identificar el riesgo al cual se enfrenta el sistema, lo que pueda pasar, consecuencias y como de probable es que pase.

Frecuencia de amenazas

Tabla 2 Frecuencia de amenazas VALOR	VULNERABILIDAD	CRITERIO

4	Muy frecuente MF		1 vez al día
3	Frecuente	F	1 vez cada semana
2	Normal	FN	1 vez al año
1	Poco frecuente	PF	Cada varios años

Tabla 2. Degradación de las Amenazas VALOR	CRITERIO	
100%	MA	Degradación muy alta del activo

80%	A	Degradación alta del activo
50%	M	Degradación mediana del activo
10%	B	Degradación baja del activo
1%	MB	Degradación muy baja del activo

Identificación y Valoración de Amenazas Tipo: Aplicaciones Informáticas

Tabla 3. Valoración de Amenazas Tipo: Aplicaciones Informáticas Activo/Amenaza	Frecuencia	Dimensión de seguridad
D	I C A	T
[E.1] Errores de los usuarios	F MA	A
[E.2] errores del administrador	FN	A
[E.4] Errores de Configuración	FN	M
[E.14] Escapes de información	PF	A
[E.18] Destrucción de información	PF A	A
[A.11] Acceso no autorizado	FN	MA

[A.15] Modificación de la información PF

Justificación de Amenazas – Aplicaciones informáticas

[E.1] Errores de los usuarios: Se presenta esta amenaza debido a que el personal no es capacitado y no es consciente del valor de los activos que manejan, teniendo un impacto en la disponibilidad muy alto.

[E.2] Errores del administrador: En la dimensión disponibilidad se le da un valor de Alto, debido a que tiene el acceso a diferentes aplicaciones, viéndose seriamente afectados, aunque la probabilidad de ocurrencia sea poco frecuente.

[E.4] Errores de configuración: Se valoró como mediana, ya que la configuración que realicen los usuarios podría presentar suplantaciones, y cierre de notas, robo de información, afectando al departamento de servicios escolares.

[E.14] Escapes de información: se valora la dimensión como Alta, ya que, si hay escape de información, ésta podría ser modificada o usada para beneficios propios, perdiendo confidencialidad y confianza institucional.

[E.18] Destrucción de información: Se consideró como una amenaza alta en disponibilidad y confidencialidad, ya que donde puedan versen afectadas los activos de información.

A.11] Acceso no autorizado: Esta dimensión es calificada muy alta, debido a la falta de capacitación del personal, pudiendo desencadenar varias amenazas como las anteriores.

[E.15] Modificación de la información: En la integridad de los datos, se calificó muy alta, debido a que la afectaría directamente. Provocando caos informático y arrojando datos erróneos a la hora de las consultas

Identificación y valoración de amenazas: Servicios.

Tabla 4. Identificación y valoración de amenazas: Servicios. Activo/Amenaza	Frecuencia		Dimensión de seguridad	
D	I	C	A	T
[E.20] Vulnerabilidades de los programas	FN		MA	
[A.5] Suplantación de la identidad del usuario	F	A	A	
[A.8] Difusión de software dañino	FN		A	
[A.24] Denegación de servicios.	PF	A	A	

Justificación de amenazas: Servicios

[E.20] Vulnerabilidades de los programas: Se consideró la probabilidad de FN (Normal) afectando la disponibilidad directamente. En caso de sufrir un ataque la amenaza se considera una suspensión de los servicios en un nivel muy alto.

[A.5] Suplantación de la identidad del usuario: Se consideró una de las mayores amenazas, ya que el personal de la institución no posee capacitación y no tiene implementado un plan de normatividad para el uso de los servicios.

[A.8] Difusión de software dañino: Dentro del nivel de frecuencia se considera normal y la dimensión de probabilidad se considera de alto grado. Debido a que los equipos en su mayoría se encuentran destinados a los estudiantes de la institución y estos no tienen concientización del uso de software licenciado.

[A.24] Denegación de servicios: se consideró poco frecuente su frecuencia de ocurrencia, pero en el nivel de degradación se considera alta, ya que se pueden presentar errores de programación, provocando el bloqueo de acceso a usuarios autorizados al sistema.

Identificación y valoración de amenazas: redes de comunicaciones.

Tabla 5. Identificación y valoración de amenazas: redes decomunicaciones Activo/Amenaza	Frecuencia			Dimensión de seguridad
D	I	C	A	T
[N.*] Desastres naturales	PF	MA		MA
[I.5] Avería de origen físico y lógico	PN			MA
[I.8] Fallo de servicio de comunicaciones	PF			A
[E.2] Errores del administrador	PF		A	A
[E.4] manipulación de configuración.				

Justificación de amenazas – redes de comunicaciones

[N.*] Desastres naturales: Se pueden llegar a presentar, debido a las condiciones geográficas rurales donde se encuentra, el cual tendría un detrimento muy alto, ya que podría causar una paralización de todas las actividades.

[I.5] Avería de origen físico y lógico: Dentro del nivel de frecuencia se considera normal, ya que por las condiciones climáticas sea amenazada, pero en la dimensión la disponibilidad se encuentra en un nivel muy alto, ya que las condiciones donde se encuentran no son las adecuadas físicamente para su protección.

[I.8] Fallo de servicio de comunicaciones: El nivel de frecuencia fue calificado como poco frecuente, pero en la dimensión de seguridad fue catalogado como alto, ya que en el momento en que falle el servicio se ve afectado por varias horas.

[E.2] Errores del administrador: La parte del administrador fue calificado como poco frecuente, pero en la dimensión de seguridad está en un nivel de degradación alto, ya que este servicio no es propio de la administración si no de la empresa que presta el servicio.

[E.4] manipulación de configuración: El nivel de frecuencia es calificado poco frecuente, pero en las dimensiones de confidencialidad y autenticidad son consideradas de alto riesgo, ya que la configuración la administra la empresa que presta el servicio.

Identificación y valoración de amenazas: Equipamiento informático

Tabla 6 Identificación y valoración de amenazas: Equipamiento informático. Activo/Amenaza	Frecuencia	Dimensión de seguridad				
	D	I	C	A	T	
[N.1] Fuego	PF	MA	MA	MA	MA	MA
[I.2] Daños por agua	PF	MA	MA	MA	MA	MA
[I.5] Avería de origen físico y lógico.	PF			A		

[E.23] Errores de mantenimiento / actualización de equipos (Hardware).	FN	A
[A.11] Acceso no autorizado	FN	A
[A.23] Manipulación de los equipos.	FN	A

Justificación de amenazas – Equipamiento informático.

[N.1] Fuego: En todas las dimensiones es considerado de muy alto impacto, ya que los equipos informáticos no cuentan con protección contra esta amenaza y no existe unas políticas establecida ante esta emergencia.

[I.2] Daños por agua: Es considerado como muy alta en degradación y poco frecuente, debido a que los equipos informáticos anteriormente fueron dañados por una granizada que ocurrió en la zona, en la cual entro agua en las instalaciones Provocando el fuera de servicio de éste.

[I.5] Avería de origen físico y lógico: La degradación se consideró alta, ya que el equipamiento informático se encuentra expuesto a la vulnerabilidad de insectos como las avispas que crean sus nidos dentro de estos equipos, como también son sometidas a largas jornadas de uso, los cuales en ocasiones el mal uso ha provocado daños físicos y lógicos.

[E.23] Errores de mantenimiento / actualización de equipos (Hardware): Es valorada con un alto impacto, debido a que los equipos de cómputo que son de control

escolar, son utilizados por los chicos de servicio social y no se cuenta con políticas de mantenimiento.

[A.11] Acceso no autorizado: En esta dimensión ésta valorada en un nivel alto, ya que no se encuentran normas de seguridad implementas y las computadoras se encuentran expuesta al acceso de cualquier persona.

A.23] Manipulación de los equipos: Esta dimensión experimenta un alto grado de degradación confidencial, ya que los equipos por parte de administración, no cuentan con políticas de seguridad y el uso exclusivo no es implementado.

Identificación y valoración de amenazas: Equipamiento auxiliar

Tabla 7. Identificación y valoración de amenazas: Equipamiento auxiliar Activo/Amenaza	Frecuencia	Dimensión de seguridad
D I C A T		
[I.5] Avería de origen PF físico y lógico.		A

Justificación de amenazas – Equipamiento auxiliar

[I.5] Avería de origen físico y lógico: Se valoró la dimensión disponibilidad en alto, debido a que no se cuenta con gabinetes para routers, switch y cables

Identificación y valoración de amenazas: Instalaciones

Tabla 8. Identificación y valoración de amenazas: Instalaciones Activo/Amenaza	Frecuencia	Dimensión de seguridad		
	D	I	C	A	T
[A.26] Ataque destructiva	PF			A

Justificación y valoración – Instalaciones

[A.26] Ataque destructiva: Se considera esta dimensión como alta, ya que no se cuentan con gabinetes, quedando expuestos y sin ninguna seguridad los equipos, por lo que cualquier persona puede tener acceso a estos

Identificación y valoración de amenazas: Personal

Tabla 9. Identificación y valoración de amenazas:	Frecuencia	Dimensión de seguridad

Personal Activo/Amenaza				
D	I	C	A	T
[E.7] Deficiencia en la organización.	FN		A	
[E.15] Alteración accidental de la FN información.		A	A	
[E.30] Ingeniería social.	F	A	A	A

Justificación y valoración – Personal

[E.7] Deficiencia en la organización: Se valoró como una degradación alta, porque no cuenta con personal calificado para implementar el Sistema de Gestión de Seguridad Informática, que se deben realizar en el departamento de servicios escolares, además no se cuenta con un cronograma de actividades para el manteniendo de equipos de cómputo en la institución.

8.3 RELACIONAR LAS AMENAZAS-VULNERABILIDADES CON LOS ACTIVOS DEFINIDOS

A continuación, se relacionan los activos presentes en el departamento de servicios escolares identificándolos y clasificándolos, tomando como guía a Metodología Magerit v3.

Tabla 10. Identificación de amenazas Activos	Amenazas
INTERNET	[A.1] Uso no previsto
OFIMÁTICA	[E.1] Errores de usuario. [E.2] Vulnerabilidades de los programas [E.2] Errores de mantenimiento / actualización de programas. [A.3] Difusión de software dañino.
ANTIVIRUS	[E.2] Difusión de software dañino [E.3] Vulnerabilidades de los programas [E.2] Errores de mantenimiento / actualización de programas.
SISTEMA OPERATIVO	[I.2] Avería de origen físico y lógico [E.1] Errores de usuario. [E.2] Difusión de software dañino.

	[E.3] Vulnerabilidades de los programas [E.3] Errores de mantenimiento / actualización de programas. [A.3] Uso no previsto

Identificación de amenazas (Continuación) Activos	Amenazas
OTROS SOFTWARE	[E.3] Difusión de software dañino [E.3] Vulnerabilidades de los programas. [E.3] Errores de mantenimiento /actualización de programas.
SERVIDOR DE BASE DE DATOS	[N.1] Fuego [N.1] Daños por agua [N.1] Desastres naturales [I.1] Contaminación medio ambiental [I.2] Avería de físico y lógico. [I.1] condiciones inadecuadas de temperatura o humedad. [E.2]Errores del administrador del sistema / de la seguridad.

	[E.1] Errores de mantenimiento /actualización de equipos. [A.3] Acceso no autorizado [A.2] Manipulación del hardware
MEDIOS DE IMPRESIÓN	[I.2] Avería de físico o lógico [I.2] Condiciones inadecuadas de temperatura o humedad. [E.2] Errores de mantenimiento. [A.2] Acceso no autorizado
COMPUTADORAS	[N.1] Daños por agua [N.1] Desastres naturales [I.1] Desastres industriales [I.3] Averías de origen físico o lógicos [I.1] Condiciones inadecuadas de temperatura o humedad. [E.1] Errores de mantenimiento / actualización de equipos. [E.1] Caída del sistema por agotamiento de recursos. [A.2] Abuso de privilegios de accesos [A.2] Uso no previsto

ROUTER	[N.1] Fuego [N.1] Dalos por agua [N.1] Desastres naturales [I.1] Contaminación medioambiental [I.1] Condiciones inadecuadas de temperatura o humedad. [E.1] Errores de mantenimiento / actualización de equipos. [A.2] Acceso no autorizado

Identificación de amenazas (Continuación) Activos	Amenazas
RED WIFI	[I.3] Fallo de servicio de comunicación [E.3] Acceso no autorizado [E.3] Errores de [re-] encaminamiento

RED LAN	[I.3] Fallo de servicios de comunicaciones [E.3] Errores de [re-] encaminamiento E 3 e [.] Errores de s cuencias [A.2] Suplantación de identidad del usuario [A.3] Acceso no autorizado
INTERNET	[A.3] Fallo de servicios de comunicación [A.3] Alteración de la información
CABLEADO	[I.1] Contaminación medio ambiental [I.1] Condiciones inadecuadas de temperatura.
MOBILIARIO	[I.1] Contaminación medio ambiental
SISTEMAS DE VIGILANCIA	[I.1] Contaminación medio ambiental [I.1] Condiciones inadecuadas de temperatura.
ANTENAS	[I.1] Contaminación medio ambiental

OTROS EQUIPOS AUXILIARES	[I.1] Contaminación medio ambiental
CD	[E.3] Alteración de la información [E.3] Fugas de información [A.3] Modificación de la información [A.3] Revelación de la información
DISCO EXTRAÍBLE	[E.3] Alteración de la información [E.3] Fugas de información [A.3] Modificación de la información [A.3] Revelación de la información
COLEGIO	[N.1] Fuego [N.1] Daños por agua [N.1] Tormentas [N.1] Terremotos [N.1] calor extremo [I.1] Desastres industriales
MANTENIMIENTO DE BASES DE DATOS	[E.2] Errores de configuración
SECRETARIA	[E.2] Enfermedad [E.2] Huelga [E.2] Extorsión

COORDINADOR	[E.2] Ingeniería social [E.2] Enfermedad [E.2] Huelga

Identificación de amenazas (Continuación) Activos	Amenazas
CORDINACIONES	[E.2] Extorsión [E.2] Ingeniería social
DIRECCION	[E.2] Enfermedad [E.2] Huelga [E.2] Extorsión [E.2] Ingeniería social
JEFE DE SISTEMA ADMINISTRATIVOS	[E.2] Enfermedad [E.2] Huelga [E.2] Extorsión [E.2] Ingeniería social
SOPORTE	[E.2] Enfermedad [E.2] Huelga [E.2] Extorsión [E.2] Ingeniería social

9. DESARROLLAR LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA BASADAS EN LA NORMA ISO 27001

9.1 ISO 27001

ISO 27001 es una norma internacional que permite el aseguramiento, la confidencialidad disponibilidad e integridad de los datos y de la información, así como de los sistemas que la procesan. Garantiza la seguridad en una organización apoya a las organizaciones a tener los activos de su información de forma segura incorpora la seguridad en el marco de gestión de la organización

Confidencialidad: trata de prevenir la divulgación no autorizada de los activos de información sobre todo cuando esta información es de carácter personal

Integridad

Garantiza que los datos permanezcan inalterados excepto cuando sean modificados por personal autorizado y esta modificación sea registrada asegurando su precisión y confidencialidad

Disponibilidad:

Es encontrar la información a disposición de quienes deben acceder a ellas ya sean personas procesos o aplicaciones.

Es una norma certificable, formaliza la gestión de la seguridad, exige al establecimiento objetivos de seguridad medibles y un criterio de mejora continua, concientiza a la organización sobre la importancia de seguridad, facilita el cumplimiento de requisitos legales y la supervivencia frente a errores o desastres o sabotajes.

Esta norma para poder implementarse en una organización necesita de una planeación y esta a su vez necesita de 4 aspectos muy importantes tales como:

- -definir la política y sistema de seguridad
- -definir el alcance del sgsi
- -elaborar un inventario de activos y un análisis de riesgos
- -definirunplandetratamientoderiesgos que incluya los controlesnecesarios
- -implementar los controles
- -operarlos y administrarlos

VERIFICAR

- Se realizan las auditorias
- -medir la eficacia
- -elaborar un plan de mejora

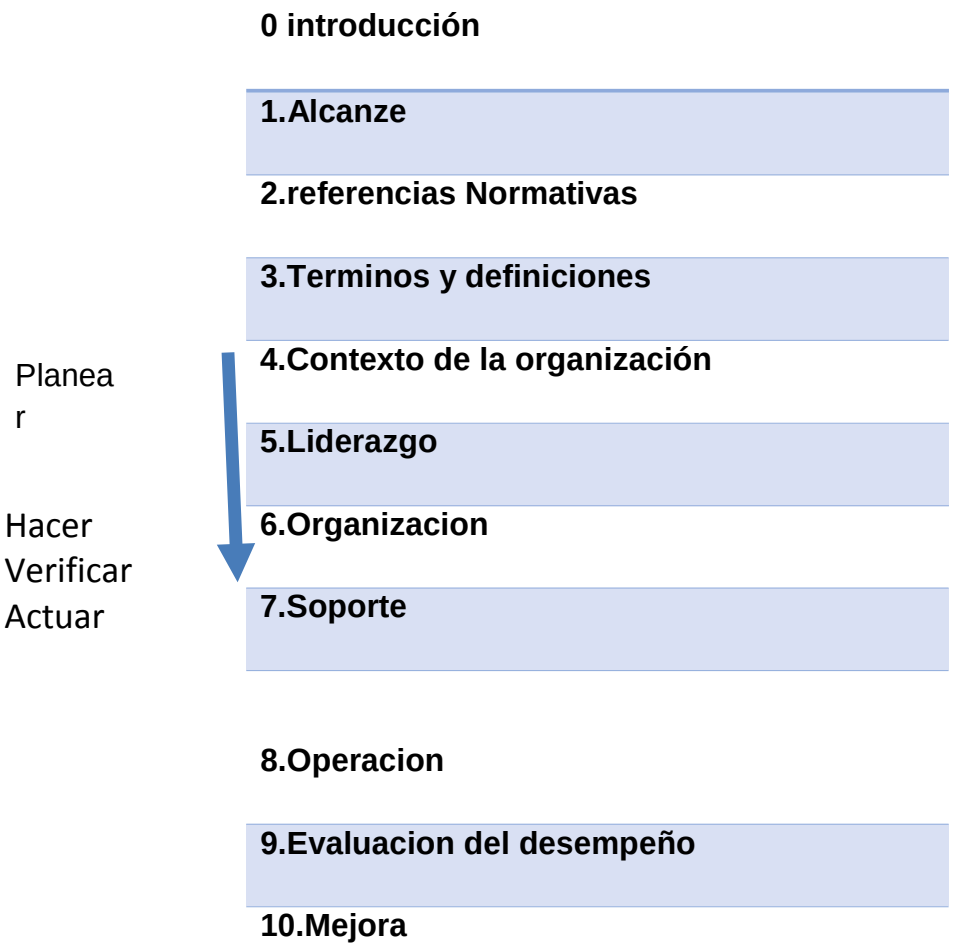
Actuar

Ejecutar el plan de mejora

Se debe mantener lo más completa posible la documentación en cada etapa de la implementación

9.2 Estructura de la norma ISO 27001

La estructura de la norma iso 27001 se compone de la siguiente manera:



Entre el punto 4 y 7 se encuentra el entendimiento de la organización y su contexto como tal a si mismo se define las expectativas de las partes interesadas y el muy importante el alcance de sistema de gestión.

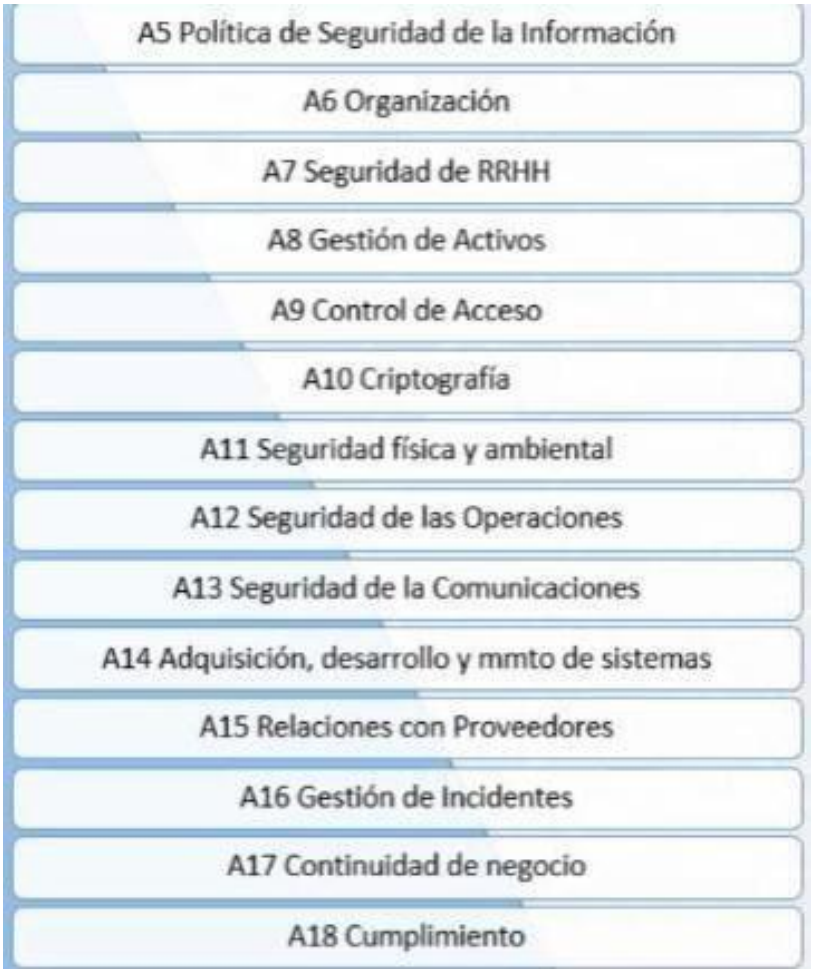
En el punto 8 se realiza la evaluación de riesgos a los activos que se hayan definido y el manejo de estos.

En la parte 9 se encuentran las evaluaciones de riesgo, el desempeño del sistema de gestión, su eficacia las auditorias, y la revisión de la dirección recordando que todo debe estar documentado.

El punto 10 es el monitoreo de sistema, la atención de las no conformidades y las acciones correctivas, así como la mejora continua que garantiza que el sistema de gestión sea idóneo y eficaz.

Todo esto es parte de lo que un auditor audita en la fase 1

En la fase 2 se encuentran 14 dominios de la norma con 114 controles, pero según su alcance abarcara todo o parcialmente estos controles:



Esta norma es un estándar básico perfecto para todas las organizaciones que quieren proteger su información es el estándar más popular en todo el mundo y es el único que se puede certificar

9.3 PROPÓSITO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El objetivo principal de la política seguridad de la información es contar con ambientes seguros, y que permita proteger los activos de información así como el uso adecuado de los recursos y gestión del riesgo para que el funcionamiento de la organización no se vea afectada.

El informe presentado a la institución, sugiere establecer las siguientes políticas, que son de interés y aplicabilidad general en todos los niveles, como en el ámbito administrativo como en el técnico.

Se desarrollaran las políticas como una serie de instrucciones, normas, estándares y prácticas establecidas, determinadas por la institución, garantizando la seguridad, confidencialidad y disponibilidad de los activos información.

El propósito de la política de seguridad informática, da soporte a la gestión, producción conservación, recuperación, información institucional, difusión de los documentos y conservación. Bajo las siguientes dimensiones de confiabilidad, integridad y autenticidad, siendo éstas de carácter indispensable para la gestión institucional.

9.4 ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El alcance establecido de acuerdo a las políticas de seguridad del departamento del Conalep debe estar ligada al programa de gestión documental desde la recepción de documentos, direccionamiento, trámite, consulta y conservación o disposición final según lo establezca la normatividad del departamento de servicios. Los documentos son un activo estratégico para poder cumplir con los objetivos y funcionalidad del departamento.

Política de seguridad institucional. Las políticas establecidas en la gestión de recursos tecnológicos propondrán y controlara el cumplimiento de las normas y políticas de seguridad, garantizando las acciones preventivas y correctivas para la salvaguarda de los equipos e instalaciones de cómputo, así como la información automatizada en general.

Para el nuevo personal de la institución deberán realizar la inducción sobre las políticas y estándares de seguridad informática, donde se les darán a conocer las obligaciones y sanciones que se puede incurrir en caso de no cumplirlas.

9.5 ¿QUÉ DEBE CONTENER LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN?

¿Qué es una política de seguridad de la información según ISO 27001 y qué debe incluir?

La política de seguridad consiste en desarrollar el marco de actuación apropiado para salvaguardar la información de la empresa. Su objetivo principal es indicar el propósito del Sistema de Gestión de Seguridad de la Información (SGSI) y del documento en sí.

Además de indicar la finalidad de la política de seguridad, se debe señalar cómo se prevé conseguirlo, cómo ha sido aprobada y cómo se realizará su seguimiento, ya que debe revisarse de forma continua. Es importante destacar que esta política tiene que adaptarse a las características de la organización, comunicarse a todos los interesados y contar con el compromiso de la alta dirección.

La cláusula 6.2 de la norma ISO 27001 establece los puntos que las organizaciones tienenque cumplir a la hora de establecer los objetivos de seguridad de la información. Uno de los más relevantes es que sean medibles, para lo cual ayudará tener presente los tres principios claves de este estándar internacional:

- Confidencialidad: solo las personas autorizadas para ello deben conocer los datos.
- Integridad: la información tiene que ser completa, válida, veraz, exacta y no estar manipulada.
- Disponibilidad: la información ha de ser accesible de forma que los usuarios autorizados para ello puedan disponer de ella cuando la necesiten y garantizar su protección.

La política tiene que adaptarse a la institución, es necesario definir un marco para establecer todos los objetivos de seguridad de la información, la política debe definir cómo se proponen los objetivos, la forma en la que se encuentran aprobados y la manera en la que se revisan.

La política tiene que mostrar el compromiso de la alta dirección para cumplir con los requisitos de todas las partes interesadas y mejorar de forma continua el Sistema de Gestión de Seguridad de la Información.

La política se debe comunicar dentro de la organización y a todas las partes interesadas, la mejor práctica es definir quiénes el responsable de tal comunicación, y entonces esa persona es responsable de hacerlo de forma continua.

La política de seguridad de la información debe ser apoyada por otras normas o procedimientos sobre temas específicos que obligan aún más la aplicación de los controles de seguridad de la información y se estructuran normalmente para tratar las necesidades de determinados grupos dentro de una organización o para cubrir ciertos temas.

- Ejemplos de estos temas de política incluyen:
- Control de acceso.
- Clasificación de la información.
- La seguridad física y ambiental.
- El uso aceptable de los activos.
- Escritorio limpio y claro de la pantalla.
- La transferencia de información.
- Los dispositivos móviles y el teletrabajo.
- Las restricciones a la instalación de software y el uso.
- Copia de seguridad.
- La transferencia de información.
- La protección contra el malware.
- La gestión de vulnerabilidades técnicas.

- Controles criptográficos.
- Las comunicaciones de seguridad.
- La intimidad y la protección de la información personal identificable.
-

Estas políticas deben ser comunicadas a los empleados y partes externas interesadas. La necesidad de normas internas de seguridad de la información varía dependiendo de las organizaciones.

Para el correcto desarrollo de los procesos del departamento de servicios, los sistemas de información deben estar protegidos adecuadamente.

Una protección fiable permite a la organización percibir mejor sus intereses y llevar a cabo eficientemente sus obligaciones en seguridad de la información. La inadecuada protección afecta al rendimiento general de toda una institución y puede afectar negativamente a la imagen, reputación de todo el plantel educativo.

.

.

El objetivo de la política es proteger los activos de información del departamento de servicios educativos en contra de todas las amenazas y vulnerabilidades internas y externas, tanto si se producen de manera deliberada como accidental.

La dirección de la institución es la responsable de aprobar una política de seguridad de la información que asegure que:

- La información estará protegida contra cualquier acceso no autorizado.
- La confidencialidad dela información, especialmente aquella relacionada con los datos de carácter personal de los empleados y alumnos.
- La integridad de la información se mantendrá en relación a la clasificación de la información.
- La disponibilidad de la información cumple con los tiempos relevantes para el desarrollo de los procesos críticos del plantel educativo.
- Los planes de continuidad de negocio serán mantenidos, probados y actualizados al menos cada año.
- La capacitación en materia de seguridad se cumple y se actualiza suficientemente para todos los empleados.

El cumplimiento de la política de seguridad de la información y de cualquier procedimiento o documentación incluida dentro del repositorio de documentación del SGSI, es obligatorio y atañe a todo el personal del plantel.

Las visitas y personal externo que accedan a las instalaciones no estarán exentas del cumplimiento de las obligaciones indiciadas en la documentación del SGSI, y el personal interno observará su cumplimiento.

. La definición del alcance es un requisito (de carácter obligatorio) descrito en la cláusula 4.3 de ISO27001, por lo que las características de este requisito tienen la intención de dejar en claro todo lo que es de interés para el sistema de gestión, relacionándose con las actividades esenciales, es decir, aquellas que permiten cumplir con la misión y los objetivos generales del departamento de servicios escolares.

El alcance precisa lo que será protegido por la organización y la magnitud de los recursos necesarios para la implementación y operación del sistema de gestión. Y debe estar disponible como información documentada

Requisitos del estándar ISO 27001 para el alcance

El estándar establece que la organización debe determinar los límites y la aplicabilidad del SGSI para definir su alcance; en este proceso, se deben considerar factores externos e internos.

Se deberán conocer todos los elementos relevantes para los propósitos del departamento de servicios escolares y plantel en general y que afectan a la capacidad para conseguir los resultados deseados con relación al Sistema de Gestión de Seguridad de la Información.

Las organizaciones y sus sistemas de seguridad de la información, se encuentran adoptando como parte de sumisión y visión, normas o metodologías, que minimicen los riesgos e inseguridades como fraudes, espionaje, sabotaje, vandalismo, incendios o inundaciones; y maximizando las inversiones y las oportunidades. Estos ataques se están volviendo más comunes

9.6 POLÍTICA GENERAL DE SEGURIDAD DE INFORMACIÓN

El departamento de servicios educativos reconoce que la información de su Propiedad, la de sus trabajadores y alumnos, así como, los activos de información y la infraestructura que la soporta, son esenciales para la continuidad de sus operaciones y para el cumplimiento de su misión y su visión; por lo que es

Fundamental protegerlos, restringiendo el acceso, uso y revelación, conforme a sus Intereses institucionales.

Políticas Generales de Seguridad de Información

1. La Dirección General debe asegurarse de que existan los recursos humanos, materiales y tecnológicos para implementar planes y programas en aspectos de seguridad de la información.

2. La Dirección General debe nombrar un Responsable de Seguridad de la Información Institucional (RSII).

3. El RSII debe establecer un Grupo Estratégico de Seguridad de la Información (GESI), que será responsable de implantar y mantener un Sistema de Gestión de la Seguridad de la Información (SGSI).

4. El RSII debe coordinar la revisión anual del cumplimiento de los objetivos y las métricas de seguridad de la información.

5. El RSII, a través del departamento de sistemas, debe verificar que se definan e implementen controles que se deriven de este Manual de Políticas de Seguridad.

6. Las Direcciones Generales Adjuntas, deben alinear sus procesos de gestión y operación, a este Manual de Políticas Generales de Seguridad de la Información.

7. El RSII, a través del departamento de sistemas, debe verificar que se desarrolle y cumpla la implementación de controles del Sistema de Gestión de Seguridad de la Información.

Conocimiento de la Política General de Seguridad de la Información

Manual de Políticas Generales de Seguridad de la Información.

Es un documento de carácter normativo, por lo que es fundamental su difusión Entre todos los colaboradores de la Institución, para su conocimiento.

Organización

Roles y responsabilidades de la seguridad de la información

En cumplimiento a la normativa externa e interna aplicable, la administración de La seguridad de la información institucional, corre a cargo del siguiente grupo de servidores públicos:

1. El Director tiene la responsabilidad de promover la seguridad de la Información Institucional.

2. El RSII, es responsable del cumplimiento de las normativas aplicables a la Seguridad de la información de la Institución.

.

3. El responsable del departamento de sistemas, es responsable de asegurar la alineación operativa de la normativa aplicable en materia de seguridad de la Información.

4. Los mandos medios y superiores de las áreas de las demás coordinaciones y Especialmente del departamento de servicios educativos, son responsables del cumplimiento de estas Políticas Generales de Seguridad de la Información.

7. Todos los colaboradores en general que presten sus servicios son responsables de conocer y cumplir las Políticas de seguridad de la información basadas en ISO 27001.

Seguridad en los Recursos Humanos

Definir las políticas que aseguren una adecuada protección de la información por Parte del personal interno y externo.

Es responsabilidad de los mandos medios y superiores de las áreas, promover y Hacer del conocimiento a todo personal a su cargo la existencia de las Políticas Generales de Seguridad de la Información.

Concientización, educación y formación en seguridad de la información

El departamento de servicios educativos en colaboración con recursos humanos deberá incluir como parte de la inducción al personal de nuevo ingreso, el material informativo necesario sobre seguridad de la información.

Gestión de activos

Asegurar la protección dela información institucional de los activos de información que la contengan.

Responsabilidad por los activos

Inventario de activos

Un activo de información, es un elemento reconocible que almacena datos, registros, información en cualquier medio y que tiene las características siguientes:

1. Es valioso por la información que contiene.

2. No es de fácil reemplazo y en algunos casos pudiera ser irrepetible.

Es responsabilidad de los mandos medios y superiores de las áreas de cada departamento identifiquen sus activos de información.

El departamento de servicios educativos, debe mantener un registro actualizado sobre los activos informáticos que soporten los servicios de las TIC

3. Hacer uso del activo únicamente para los propósitos y actividades de la Institución.

4. Reportar cualquier incidente o problema relacionado con el activo de información.

5. Cualquier omisión (con dolo o involuntaria) de reportar algún incidente relacionado a cualquier activo bajo su guarda y custodia, se considera una falta hacia la seguridad de la información que en su caso debe reportarse a las autoridades competentes.

6. Realizar lo necesario para mantener el activo de información en buenas Condiciones que garantice y cumplan su función.

El departamento de servicios educativos deberá trabajar en conjunto con el departamento de sistemas der para proporcionar los servicios necesarios para asegurar el manejo de la información

Está restringido el uso de medios removibles de almacenamiento, por lo que se deshabilita la funcionalidad de los puertos USB y unidades ópticas de grabación en todos los equipos de cómputo institucionales; la autorización de uso de los medios removibles debe ser tramitada, justificada y autorizada por la dirección del solicitante, con el visto bueno de quien este como responsable..

El RSII, a través del departamento de sistemas, debe concientizar sobre el buen uso y mejores prácticas del manejo de medios removibles de almacenamiento, para el traslado de la información.

Eliminación de medios

El departamento de sistemas debe contar con procedimientos seguros que garantice el traslado de los medios de información, mediante un mecanismo auditable; mismo que puede ser verificado por El RSII, a través del departamento de sistemas

Control de accesos

Política de control de acceso

El RSII, a través del departamento de sistemas debe establecer controles de seguridad para la Gestión de Cuentas de Usuarios en el departamento de servicios educativos y en todo el plantel.

Asegurar que sólo usuarios autorizados accedan a los servicios de información y que lo hagan a través de privilegios adecuados a su perfil o rol en la Institución

Control de acceso a las redes y servicios asociados

1. Los controles de acceso a los servicios de información, deben asignarse con base en los roles y perfiles de los usuarios, según el servicio requerido.

2. La autentificación de usuarios, debe hacerse a través de canales cifrados y haciendo uso de contraseñas encriptados .

Gestión del acceso a usuarios

Gestión de altas/bajas/cambios en el registro de usuarios

Todos los aplicativos y servicios TIC institucionales deben tener un registro de altas, bajas y cambios siguiendo lo dispuesto en el proceso de Gestión de Cuentas de Usuario, descrito en las Directrices de Gestión de Cuentas de Usuario.

Gestión de los derechos de acceso asignados a usuarios

Todos los accesos a servicios TIC y aplicativos deben ser asignados de acuerdo a su función, mediante roles y perfiles, propiciando una correcta segregación de funciones.

Gestión de derechos de acceso con privilegios especiales

Los usuarios con privilegios especiales de acceso, deben contar con la autorización del responsable del activo.

Las cuentas de usuarios con privilegios especiales de acceso deben ser diferentes a las cuentas que utilizan para la operación.

Gestión de información confidencial de autenticación de usuarios

El departamento de sistemas debe asegurar la confidencialidad de la entrega de contraseñas en todos sus procesos.

Revisión de los derechos de acceso de usuarios

Los derechos de acceso de los usuarios deben ser revisados anualmente por la Gerencia de Seguridad de la Información.

Retirada o adaptación de los derechos de acceso

Es responsabilidad de la Dirección de Recursos Humanos, notificar las bajas o cambios de adscripción del personal, al departamento de sistemas, para la ejecución del cambio o remoción de los derechos de acceso.

Es responsabilidad de los mandos medios y superiores de las áreas que cuenten con personal externo, que tengan acceso a los servicios TIC y a los aplicativos Institucionales, notificar las bajas o cambios defunciones del personal, ala Gerencia de Seguridad de la Información, para la ejecución del cambio o remoción de los derechos de acceso.

Responsabilidades del usuario

Uso de información confidencial para la autenticación

Todo el personal responsable de su contraseña, la cual es confidencial y debe mantenerse secreta.

Para hacer uso de la infraestructura tecnológica, los usuarios deben aceptar los términos y condiciones de la Política de Uso Aceptable de Aplicativos y Servicios Tecnológicos Institucionales.

El usuario debe cambiar la contraseña inicial, después de que le fue asignada al sistema o aplicativo, mismo que debe estar configurado para que esto sea de forma automática.

Solo deben tener acceso a los aplicativos institucionales los usuarios autorizados, con la cuenta asignada para tal efecto; en ningún caso deben acceder usando una cuenta diferente.

Control de acceso a sistemas y aplicaciones

Restricción del acceso a la información

El departamento de sistemas debe asegurar que las aplicaciones cuenten con un control de acceso centralizado, donde el usuario debe ser identificado con un user-id y una contraseña segura.

La administración de los derechos de acceso a los aplicativos, directorio activo y bases de datos institucionales, se realiza mediante roles y/o perfiles.

Todos los usuarios con acceso a los aplicativos institucionales deben identificarse en forma única y contar con los derechos de acceso asignados previamente, de acuerdo a su rol y perfil.

Seguridad física y ambiental

Asegurar que sólo usuarios autorizados tengan acceso a las instalaciones de procesamiento de información, para prevenir cualquier daño físico o interferencia con los equipos o la instalación.

Áreas seguras

Perímetro de seguridad física

El RSII, a través del departamento de sistemas y en conjunto con la Dirección de Recursos Materiales, debe informar al GESI la designación de las áreas seguras de la Institución.

La Dirección de Recursos Materiales y el departamento de sistemas son responsables de definir un espacio físico seguro, que cumpla con lo mínimo para asegurar el procesamiento y almacenamiento de la información.

Se deberán de implementar los mecanismos necesarios que permitan limitar el acceso a las áreas seguras, solamente para el personal autorizado

No se permitirá el acceso a las áreas seguras al personal que no esté expresamente autorizado.

Es responsabilidad de las personas autorizadas a las áreas restringidas, permitir el acceso al personal ajeno a éstas.

Control físico de entrada

Las áreas seguras deben contar con mecanismos de ingreso que consideren la autorización, registro y validación de los accesos.

Seguridad de oficinas y recursos

Se debe proporcionar a cada empleado un espacio físico asignado que cuente con mobiliario protegido para el resguardo de información física.

Se debe proporcionar a cada empleado un acceso controlado para el uso de las instalaciones de acuerdo a sus funciones dentro de la Institución, el acceso a áreas restringidas debe ser autorizado por la dirección responsable del área restringida.

Protección contra amenazas externas y ambientales

Las áreas de acceso a las instalaciones, deben ser controladas y debe restringirse el acceso a las áreas seguras para evitar el acceso no autorizado.

Seguridad de los equipos

Ubicación y protección de equipos

Todo equipo que almacene, procese o transmita información esencial debe ser protegido para disminuir el riegos de amenazas ambientales o físicas; tales como, inundaciones, rayos, sismos, radiaciones, polvo, humedad, vandalismo, explosión, humo etc.

La Institución debe contar con un centro de datos primario, que garantice la protección de los equipos que soportan los procesos institucionales, así como, los servicios de soporte.

Además, debe contar con un centro de datos secundario, cuya ubicación geográfica sea diferente del centro de datos primario, que garantice la continuidad de las operaciones, ante una contingencia.

Todos los equipos de soporte que se encuentran fuera de los centros de datos, deben estar ubicados y protegidos en áreas restringidas, de acuerdo a las especificaciones del fabricante.

Sistemas de aire acondicionado de precisión redundante y adecuada, para tener una temperatura idónea para el correcto funcionamiento de los equipos y prevenir fallas.

Unidades de alimentación ininterrumpida (UPS), redundante.

Alarmas de detección de humo y sistemas automáticos de extinción de fuego.

Extintores y equipo contra incendio con capacidad de detener el fuego generado por equipo eléctrico.

Contar con un control de acceso sólo para personal autorizado.

Instalaciones de suministro

Las instalaciones de procesamiento de información que opera la Institución, debe contar con equipos que suministren de energía eléctrica de forma ininterrumpida por al menos 24 horas, tales como generadores y UPS, así como, sus procedimientos documentados en caso de contingencia.

Seguridad en cableado

El cableado debe cumplir con las especificaciones del fabricante para minimizar errores físicos. No debe estar expuesto a condiciones ambientales que aceleren su deterioro, tales como: agua, corrosivos, exceso de calor, etc.

Todo el cableado de datos debe estar debidamente etiquetado en los paneles de parcheo y adecuadamente instalado, para facilitar su mantenimiento. Cuando exista un cambio en el cableado, se debe actualizar la memoria técnica correspondiente.

El cableado de datos y de energía debe estar separado en distintitas canaletas o ductos, para evitar interferencias, siguiendo las normas aplicables.

El acceso a los cuartos donde residan los paneles de parcheo y tableros de distribución eléctrica, deben ser restringido al personal responsable de la red y del soporte técnico o mantenimiento de la misma.

Mantenimiento de los equipos

Todo activo de información debe contar con programas de soporte y mantenimiento, para su correcto funcionamiento y disponibilidad.

El departamento de servicios educativos debe validar que los mantenimientos que se lleven a cabo, sean realizados por personal capacitado, de acuerdo a las especificaciones del fabricante. Asimismo, asegurarse que se conserve un registro de todos los mantenimientos preventivos y correctivos efectuados.

Salida de activos

El departamento de servicios educativos debe establecer un procedimiento para el registro de entrada y salida de equipos de cómputo (internos y externos).

Seguridad de los equipos y activos fuera de las instalaciones

Todo equipo que almacene, procese, transmita información crítica debe operar dentro de las instalaciones de la Institución o de las contratadas para tal efecto.

El departamento de servicios educativos debe establecer un procedimiento que asegure que la información y/o configuraciones no queden expuestas.

.

Los equipos de cómputo móviles (laptops) deben ser protegidos con las medidas y mecanismos de seguridad de la información, con los que cuente la Institución.

Los equipos de cómputo móviles (laptops) que se encuentran fuera de las instalaciones y requieran conectarse a la red interna de solo podrán realizarlo por medio del cliente de VPN institucional.

Reutilización o baja de dispositivos de almacenamiento

El departamento de servicios educativos, debe contar con un proceso de baja o devolución, que confirme el borrado seguro de la información en los activos y el departamento Seguridad de la Información verificara aleatoriamente la ejecución de este proceso.

Equipo informático de usuario desatendido

El departamento de servicios educativos debe implementar en todo equipo informático las configuraciones necesarias para su bloqueo de forma automática en un tiempo máximo de 5 minutos, una vez que éste se encuentre desatendido.

Política de escritorio seguro y bloqueo de pantalla

Todo el personal que debe cumplir con los siguientes lineamientos al ausentarse de su lugar de trabajo o finalizar su jornada laboral:

En caso de contar con puerta, cajones o archiveros, éstos deben cerrarlos con llave.

Retirar del escritorio cualquier tipo de información, sin importar el medio en que se encuentre (papel, post-its, discos, medios magnéticos) y resguardarla en gabinetes con llave o cualquier otro mueble con acceso controlado.

Destruir de manera segura aquella información que ya no será utilizada.

No dejar documentos con información sobre impresoras, copiadoras, etc.

No utilizar la información impresa que sea confidencial o de uso restringido para reciclaje

9.7 POLÍTICAS DE SEGURIDAD EN LAS OPERACIONES

Políticas de seguridad en las operaciones

La presente Política tiene por objetivo salvaguardar la confidencialidad, integridad y disponibilidad de la información que se procesa mediante los distintos mecanismos de comunicación y operación de los sistemas de información.

Responsabilidades y procedimientos de operación

Documentación de procedimientos de operación

Los procedimientos de operación y los procesos de todas las áreas de la Institución, deben documentarse en manuales de operación de acuerdo a lo establecido en el documento de Objetivos y Lineamientos del Sistema de Control Interno.

El departamento de servicios educativos es responsable de documentar sus procedimientos y de contar con memorias técnicas para la administración de los aplicativos y sistemas de información, mismos que deben estar actualizados y vigentes.

Administración de cambios

El departamento de servicios educativos debe establecer un proceso documentado para la administración de cambios en los ambientes operativos.

El Proceso de Administración de Cambios debe contar con un grupo de trabajo, facultado para promover, identificar y evaluar cuando se requiera un cambio en la infraestructura tecnológica de la Institución; este grupo debe sesionar al menos una vez al mes para informar los cambios realizados o en proceso.

En este grupo debe participar al menos un representante del departamento de sistemas

Todo cambio o modificación de los datos en las bases de datos productivas, deben contar con el visto bueno del director responsable del aplicativo o responsable funcional con nivel jerárquico inferior inmediato.

Controles contra el código malicioso

El departamento de servicios educativos debe asegurar que todos los equipos de escritorio, móviles (laptops) y servidores utilizados en la red de la Institución, tengan instalado el software antivirus, anti-malware, anti-xploits, anti-spam y anti-spyware institucional y mantenerlo actualizado, tanto en versión como en definición de firmas.

Así mismo, deben cumplir con una configuración base de parches de seguridad.

Los proveedores o personal externo que tengan equipos y que necesiten conectarse a la red de la Institución, deben contar con un software de antivirus autorizado por el departamento de sistemas.

El software de antivirus anti-malware, anti-xploits, anti-spam y anti-spyware institucional debe permitir como mínimo:

1. Ejecutar búsqueda automática, manual o programable.

2. Limpiar archivos infectados.

3. Mantener en cuarentena los archivos que no puedan ser limpiados.

4. Contar con mecanismos para prevenir y contener amenazas, así como, negación de servicios.

5. Proveer la capacidad de actualizaciones automáticas y programables.

6. Registrar los incidentes de virus y contar con la capacidad de análisis de registro.

7. Detectar código malicioso.

8. Generar alertas.

9. Llevar una administración centralizada.

El software contra código malicioso y sus componentes deben ser actualizados cuando exista una nueva versión o definición de firmas, con base a los contratos con el fabricante.

El departamento de servicios educativos debe dar acceso al RSII y al departamento de sistemas de los reportes mensuales detallando las incidencias detectadas por el antivirus.

Respaldo y borrado de información

Respaldo de información

Todos los mandos medios y superiores de las áreas dentro de la Institución, son responsables de identificar la información que sea sensible para la operación de su área de acuerdo a su criticidad y deben dar aviso al departamento de sistemas para gestionar su respaldo y periodicidad.

El departamento de servicios educativos debe:

1. Implementar procedimientos para respaldar la información de la Institución.

2. Respaldar periódicamente toda la información (configuraciones, logs, file systems, bases de datos, etc.) que resida en los sistemas de la Institución, considerando su criticidad.

3. Asegurar que el respaldo de la información de los sistemas, en lo posible no degrade su operación.

4. Los respaldos deben llevarse a cabo preferentemente fuera de los horarios de operación y se documentan las excepciones.

5. Proveer espacios suficientes para almacenamiento y resguardo de la información del negocio que será respaldada periódicamente, siendo responsabilidad de cada usuario el manejo de la información a respaldar.

6. Revisar y validar periódicamente la información respaldada, para evitar que se pierda, se vuelva obsoleta o se deteriore; asegurando que la información sea recuperable y que cumple con los principios de integridad y disponibilidad.

7. Evitar que los medios de respaldo utilizados para el almacenamiento de información se vuelvan obsoletos. En la medida de lo posible, debe utilizar tecnologías de punta que permitan reducir el espacio físico que ocupan estos medios.

8. Almacenar los respaldos generados en un sitio protegido contra el medio ambiente y con controles estrictos de acceso, que debe ubicarse a una distancia razonable fuera del alcance de un evento en la zona principal.

9. Mantener un registro actualizado, con acceso controlado, que contenga los datos de todos los archivos respaldados, fuera de las instalaciones de la Institución, indicando la fecha más reciente en que la información fue modificada y la naturaleza de la misma

Almacenamiento de información

El departamento de sistemas debe proporcionar y administrar espacio de almacenamiento suficiente para que las áreas puedan resguardar copia de su

información institucional. Asimismo, debe contar con un inventario de usuarios autorizados en los recursos de almacenamiento de cada área.

Queda prohibido la utilización de recursos de almacenamiento institucional para archivos de uso personal o de diversión.

El departamento de sistemas debe contar con procedimientos y mecanismos de borrado o destrucción y de la información de la Institución, que ya no sea necesaria, ni por la operación, ni por requerimientos legales.

Toda la información que ya no sea utilizada se debe eliminar de forma segura, de acuerdo a los criterios que establezcan las áreas responsables de la información.

Control de software en sistemas operacionales

Instalación de software

El departamento de servicios debe asegurarse que todo el software que se instale en los servidores y equipos de cómputo personal cuente con el licenciamiento vigente, suficiente para atender los requerimientos del departamento

.

El departamento de sistemas es responsable de administrar y resguardar las licencias del software institucional.

Todo el software que se instale en ambientes productivos debe ser previamente evaluado y probado en ambientes de pruebas. La instalación del software autorizado debe ser realizada por personal calificado, siguiendo los lineamientos de control de cambios y llevando un control estricto de las versiones.

Todo el software que se instale en los equipos de cómputo debe estar inventariado en un catálogo de software institucional.

El departamento de sistemas es la única instancia autorizada para instalar, actualizar y desinstalar el software de los equipos de cómputo.

Gestión de la vulnerabilidad técnica

Gestión de las vulnerabilidades

La Institución a través del departamento de sistemas debe establecer el alcance de las evaluaciones que se realicen

Para identificar vulnerabilidades enel hardware, software, sistemas, aplicaciones, seguridad, recuperación de información y redes.

.

El departamento de servicios educativos, debe documentar el seguimiento a las acciones de mejora, para solventar las vulnerabilidades detectadas, siguiendo el plan de remediación propuesto en las políticas de seguridad de información.

Las restricciones a la instalación de software

Queda prohibido al personal no autorizado instalar y/o ejecutar software para explorar (escanear)redes, equipos de cómputo ysistemas de información, en busca de protocolos, puertos, recursos compartidos y vulnerabilidades; así como, el descubrimiento y monitoreo no autorizado del tráfico de la red de la Institución. El departamento de sistemas debe implementar mecanismos para restringir la instalación de software no autorizado.

Consideraciones de las auditorías de los sistemas de información

Todos los sistemas deben contar con un registro de auditoría, que permita identificar la manera en que trabaja la institución-

.

Controles de auditoría de los sistemas de información

Las actividades de auditoría que involucren la revisiones de sistemas y aplicativos institucionales, deben ser calendarizadas y planeadas para prevenir interrupciones en la operación, con un perfil de consulta y un estado de inhabilitado hasta su requerimiento por parte de quien realizara la auditoria.

El departamento de sistemas, será quien autorice la activación de los usuarios de auditoría en cada revisión, con previo conocimiento del alcance y su temporalidad.

Seguridad de las comunicaciones

Asegurar la protección de la información en las redes y de las instalaciones de soporte dentro de la organización y con terceros.

Gestión de seguridad de red

Controles de red

El departamento de sistemas es responsable del diseño, implementación, establecimiento, contratación, administración, mantenimiento y soporte de las redes de voz y datos y de toda la infraestructura de comunicaciones que las soportan.

El departamento de servicios educativos debe implementar procedimientos y controles tecnológicos para asegurar la integridad, disponibilidad y confidencialidad de la información, en su transmisión en las redes e infraestructuras de comunicaciones de la Institución.

El departamento de sistemas debe establecer los requerimientos técnicos para la conexión a la red y sus servicios.

La institución debe contar con la infraestructura necesaria para la protección de la información y sus activos tecnológicos, así como, para el monitoreo y detección oportuna de incidentes de seguridad.

El departamento de sistemas debe implementar mecanismos para el uso del servicio de internet en la Institución, la cual debe contar con herramientas de seguridad y de filtrado de contenido, que permitan la segmentación de navegación conforme a la operación de las áreas.

El uso de servicio de internet se considerará con el mínimo acceso y sólo se podrá requerir un mayor acceso mediante una solicitud debidamente justificada, requisitada y autorizada por el director del área, quien será responsable de verificar el buen uso del servicio requerido.

El departamento de sistemas debe proteger la información que de estos servicios que se deriven, mediante la correcta configuración de los servidores y/o dispositivos sobre los que operan estos servicios.

Seguridad de los servicios de red

El departamento de sistemas debe implementar:

- Mecanismos que midan y aseguren niveles de disponibilidad y tiempos de respuesta, que garanticen la adecuada ejecución de las operaciones y servicios bancarios que se realizan.
- Medidas de control que aseguren la protección y confidencialidad de la información, generada por la realización de operaciones bancarias, a través de cualquier medio tecnológico.

Se debe llevar a cabo revisiones periódicas de conexiones externas, tomando en consideración los siguientes puntos:

1. Vigencia

2. Dueño de la conexión externa por parte de la Institución

3. Descripción de la conexión externa

4. Uso de la conexión externa

5. Arquitectura de seguridad

La administración e infraestructura debe estar clasificada en zonas de seguridad, basadas en funciones, tipo de datos y requerimientos de acceso a los espacios de almacenamiento.

Se deben utilizar mecanismos de autenticación y cifrado para la protección de la comunicación inalámbrica.

Requerimientos de seguridad

El plantel en general debe cuidar el cumplimiento de los requerimientos de seguridad mínimos para cada elemento de la red institucional, entre ellos:

1. Zonas:

I. Zona de acceso - debe contar con, al menos, los siguientes controles de seguridad:

a. Acceso desde internet:

Firewall

Sistema de Prevención de Intrusiones (IPS)

Servidor de VPNS, en caso de acceder a servicios de red internos

Servidor de autenticación de dominio

Acceso hacia internet

Filtrado de contenido

II. Zonas de distribución - debe contar

Con al menos los siguientes controles:

a. Listas de Control de Acceso (ACL), en ruteadores y switches

III. Zona interna - debe contar al menos con los siguientes controles de seguridad:

a. Listas de Control de Acceso (ACL), en ruteadores y switches

b. Sistema de Prevención de Intrusiones (IPS)

IV. Zona centro o núcleo - debe protegerse por los siguientes controles de seguridad:

a. Firewalls

b. Sistema de Prevención de Intrusiones (IPS)

c. Antivirus

2. Requerimientos de protección para segmentos que transmitan información confidencial:

Todos los segmentos de red que transmitan información confidencial,deben hacerlo de forma encriptadas. Ya sea con encriptación de punto a punto, o bien, mediante la encriptación de la información en sí.

3. Requerimientos para el monitoreo de los elementos y dispositivos de red:

Es necesario que la red y los dispositivos que la componen se monitoreen de forma regular, con la finalidad de identificar de manera oportuna problemas de desempeño que pudieran estar relacionados con incidentes de seguridad.

4. Configuración de dispositivos de red:

Para el cumplimiento de esta política de seguridad en red, la Dirección de Tecnologías y Comunicaciones debe definir configuraciones seguras para cada tipo de dispositivo que integra la red y debe aplicar a todos los dispositivos que la componen. Es necesario que dichos estándares tomen como referencia la información sobre vulnerabilidades y las especificaciones de los fabricantes para integrar la configuración segura.

5. Requerimientos de seguridad física para cableado y dispositivos de red:

El cableado de la red de datos debe cumplir con las especificaciones del fabricante, para minimizar errores físicos en la red. No debe estar expuesto a condiciones ambientales que aceleren su deterioro, tales como: agua, corrosivos, exceso de calor, etc.

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

La Dirección General Adjunta de Administración de Riesgos, coordinara en conjunto con las Direcciones de la Institución la generación de un plan de acción para mantener la continuidad de los procesos, operaciones y servicios críticos de la institución educativa; lo anterior, para casos de contingencias provocados por acciones deliberadas, accidentales, fallas de los sistemas o desastres naturales.

Continuidad de la seguridad de la información

Planificación de la continuidad de la seguridad de la información

Se debe nombrar a un responsable para la coordinación del plan de continuidad del negocio u organización, en caso de un desastre, de acuerdo a lo establecido en el “Manual de Políticas y Procedimientos de Continuidad del Negocio”.

El coordinador del plan de continuidad debe mantener una estrecha comunicación

con las áreas directivas, operativas, tecnológicas, personal de seguridad física y Protección Civil.

El departamento de sistemas debe proporcionar soluciones y servicios tecnológicos que permitan la redundancia para los procesos contemplados en el plan de recuperación de la Institución.

Implantación del plan de la continuidad de la seguridad de la información

Todas las Direcciones Generales Adjuntas a través de sus Direcciones responsable de procesos sustantivos y de apoyo, deben contar con una estrategia de recuperación documentada y validada, siguiendo el “Manual de Políticas y Procedimientos de Continuidad del Negocio”.

La Gerencia de Seguridad de la Información debe validar que los planes de continuidad reciban mantenimiento, esto de acuerdo al marco de referencia establecido

Cumplimiento

Coadyuvar al cumplimiento de los requerimientos legales, contractuales o regulatorios a los que está sujeto la institución educativa ; así como, fomentar la revisión y seguimiento a eventos que provoquen una interrupción total o parcial de los servicios prestados, evitando violaciones de cualquier ley, obligación reguladora o contractual y de cualquier requerimiento de seguridad.

Cumplimiento con requerimientos legales y contractuales

Identificación de normativa aplicable y requisitos contractuales

Es responsabilidad del departamento de sistemas que se definan las políticas que coadyuven al cumplimiento de los requerimientos regulatorios en materia de seguridad de la información.

El departamento de servicios educativos debe coordinarse con los responsables de la administración de los servicios de TIC y con aquellos responsables de la operación de los mismos, a fin de que los acuerdos de nivel de servicio y los acuerdos de nivel operacional sean determinados y considerados en función de los programas de continuidad y de contingencia.

Derechos de propiedad intelectual

El departamento de sistemas, en coordinación con los responsables de las soluciones e infraestructuras tecnológicas de la Institución, debe validar uso de licencias y cumplimiento con los derechos de autor de toda aplicación y herramienta

de software utilizada en las estaciones de trabajo. Todo el software instalado en las computadoras de la Institución debe ser legal.

Para cualquier desarrollo y en su caso mantenimiento de aplicativos de cómputo, se debe propiedad intelectual, a través del registro correspondiente, en el que se incluyan la totalidad de los componentes del aplicativo de cómputo de que se trate, como son: el código fuente, el diseño físico y lógico, los manuales técnicos y de usuario.

Protección de los registros.

El departamento de sistemas debe asegurar que cada operación o actividad realizada por los usuarios de los aplicativos institucionales o sistemas, deje constancia electrónica, conforme a registros de auditoría.

El departamento de sistemas debe instrumentar condiciones de seguridad, que impidan borrar o alterar los registros de auditoría y las bitácoras de seguridad de los sistemas.

Privacidad y protección de la información de identificación personal

Uno de los objetivos de la seguridad de la información es la protección de datos del alumno en cualquier forma. Dichos datos son custodiados por una serie de controles físicos y lógicos para impedir algún daño a su confidencialidad, integridad y disponibilidad.

Adicionalmente, la Ley Federal de Protección de Datos Personales en Posesión de Particulares y su Reglamento es aplicable para la Institución, motivo por el cual la institución educativa debe implementar los controles necesarios para preservar la confidencialidad, integridad y disponibilidad de los siguientes datos personales:

1. Datos personales de los alumnos

2. Datos personales de los empleados de la Institución.

Esta información es catalogada como confidencial dentro del esquema de clasificación de la información adoptado por la Institución, y su trato es con base a los lineamientos de la entidad emisora de dicha Ley y su Reglamento en materia de protección de datos personales y en coordinación con los alumnos

.

El RSII, a través del departamento de sistemas, da seguimiento a los análisis, actividades y resultados que se deriven de las revisiones realizadas.

Cumplimiento de las normas y políticas de seguridad

El personal que labora en la Institución, tiene la obligación de adoptar cualquier regulación en materia de seguridad de la información, que sea aplicable a la Institución, o bien, cualquier normatividad que sea aprobada.

Revisión del cumplimiento con normatividad relacionada con TIC

Las actividades de auditoría que involucren la revisiones de sistemas, aplicativos institucionales, deben ser calendarizadas y planeadas para prevenir interrupciones en la operación.

Los permisos de acceso a los sistemas o aplicativos institucionales del personal de la Dirección de Auditoría, deben ser solo de consulta y estar inactivos; se activarán por ejercicio o revisión, el RSII a través del departamento de sistemas será quien autorice la activación de dichos usuarios.

Los requerimientos y el alcance de las revisiones, serán acordados con el RSII, a través del departamento de sistemas.

9.8 INFRACCIONES A LAS POLÍTICAS DE SEGURIDAD

1. Se considera como falta a las Políticas del Seguridad de la Información lo siguiente:

a) la falta de firma a los acuerdos de confidencialidad y responsabilidad de activos sensibles de información.

b) que los activos de información no se encuentren actualizados

c) hacer caso omiso a los incidentes de seguridad o las violaciones a las políticas de seguridad, cuando se infrinja alguno de ellos se tendrá que reportar y documentar

d) no seguir el protocolo de seguridad de la información cuando se encuentre fuera de su área de trabajo o al terminar la jornada laboral.

e) olvidar y dejar información en carpetas compartidas, no autorizadas o en lugares distintos al servidor de archivos institucional, permitiendo el acceso a ellas a cualquier persona.

f) no dejar bien cerrado bajo llave sus escritorios o estantes de trabajo.

g) dejar que personas ajenas a la Institución, se introduzcan en el interior de las instalaciones, en áreas prohibidas para personas no autorizadas.

h) cuando alguien solicite contraseñas de otro usuario

j) Utilizar password de acceso de un usuario distinto al propio para ingresar a los sistemas o aplicaciones.

2. Uso indebido de la plataforma tecnológica institucional:

a) Hacer uso de la red de datos institucional, para acceder, almacenar, mantener o difundir en o desde los equipos institucionales, material con contenido sexual u ofensivo, cadenas de correos y correos masivos no autorizados.

b) La utilización de software no relacionado con la actividad laboral que pueda degradar el desempeño de la plataforma tecnológica institucional.

c) Actuar con negligencia en el cuidado de los equipos, dispositivos portátiles o móviles entregados para actividades propias

d) Conectar equipos de cómputo personal u otros sistemas electrónicos personales a la red de datos institucional, sin la debida autorización.

e) El utilizar los recursos tecnológicos institucionales para beneficio personal.

f) Instalar programas o software no autorizados en las estaciones de trabajo o equipos portátiles institucionales, cuyo uso no esté autorizado por el departamento de sistemas

3. Son acciones de sabotaje de la plataforma tecnológica institucional:

a) Impedir u obstaculizar el funcionamiento de las aplicaciones, bases de datos o a las redes de telecomunicaciones y datos de la institución, sin estar autorizado.

b) Destruir, dañar, borrar, deteriorar activos informáticos de la institución sin autorización.

c) Distribuir, enviar, introducir software malicioso u otros programas de computación de efectos dañinos en la plataforma tecnológica

d) Alterar datos personales de las bases de datos institucionales.

e) Realizar cambios no autorizados en la plataforma tecnológica de la institución.

4. acciones de acceso no autorizado a la infraestructura tecnológica

a) Acceder sin autorización expresa a todo en parte a los sistemas de la institución.

b) Suplantar a un usuario ante los sistemas de autenticación y autorización establecidos.

c) No mantener la confidencialidad de las contraseñas de acceso a la red de datos, los recursos tecnológicos o los sistemas de información o permitir que otras personas accedan con el usuario y clave del titular a éstos.

d) Otorgar el acceso o privilegios a la infraestructura a personas no autorizadas.

e) Ingresar a carpetas sin autorización.

5. Son acciones de robo de información:

a) Ejecutar acciones tendientes a eludir o variar los controles establecidos por la institución

b) Retirar de las instalaciones de la Institución, estaciones de trabajo o equipos portátiles que contengan información institucional, sin la autorización pertinente.

c) Sustraer de las instalaciones

documentos con información institucional, o abandonarlos en lugares públicos o de fácil acceso.

9.9 ¿CUÁLES SON LOS BENEFICIOS DE LA CERTIFICACIÓN ISO 27001 Y COMO OBTENERLA?

La Certificación ISO 27001 de Seguridad de la Información proporciona un marco de gestión para la Seguridad de la Información aplicable para cualquier tipo de organización, pública o privada, grande o pequeña.

Iso 27001 ofrece un marco para identificar todos los requisitos y definir una manera sistemática de cumplir con todos ellos además la mayoría de la legislación de seguridad de la información se basa en ISO 2701 al obtenerse una certificación las compañías brindan una prueba (emitida por un organismo de certificación) de que protegen información de acuerdo con el estándar internacional.

El trabajo que realiza un auditor para entregar la certificación basada en ISO 27001 será el de revisar toda la documentación, hacer preguntas y buscar todas la pruebas que certifiquen que se cumplen todos los requisitos que establece la norma ISO 27001.

La norma ISO 27001 establece una serie de requisitos, que la empresa tiene que cumplir. Para comprobar que se cumple con lo que dice la norma, el auditor debe examinar todos los procedimientos, los registros, las políticas de seguridad y las personas. Las personas serán estudiadas por la realización de entrevistas personales en las que las preguntan que se lleven a cabo irán encaminadas a conocer que el Sistema de Gestión de Seguridad de la Información se encuentra implantado en la organización según la norma ISO 27001.

Para los trabajadores de la empresa es muy interesante conocer cómo piensan los auditores que participan en la auditoría de certificación.

Documentación obligatoria

El auditor que certifique el Sistema de Gestión de Seguridad de la Información según la norma ISO 27001 debe realizar una revisión de toda la documentación que existe, se pueden pedir todos los documentos que establece la norma ISO 27001. En el caso de los controles de seguridad, se utiliza la Declaración de Aplicabilidad cómo guía. Existe una serie de documentos que son obligatorios y que se establecen gracias a la norma ISO 27001.

Además de los documentos obligatorios, existen otros documentos que pueden ayudar a implementar el Sistema de Gestión de Seguridad de la Información y el auditor debe revisar todos estos documentos.

Evidencias

Una vez que se ha comprobado la existencia de los documentos del Sistema de Gestión de Seguridad de la Información tiene que continuar y el siguiente paso será verificar que todo lo que se encuentra escrito en los documentos se corresponden a la realidad.

Podemos poner el siguiente ejemplo: la empresa define que la política de seguridad de la información se debe revisar cada año. El auditor puede preguntar si se ha revisado la política de seguridad pero no puede fiarse sólo de la palabra sino que tiene que ser comprobado, por lo que necesitan pruebas. La evidencia puede estar incluida en los requisitos, en las actas de reunión, etc. La siguiente pregunta puede ser que le muestre los registros en los que aparece la fecha en la que se realizó la revisión de la política de seguridad de la información.

Los controles de seguridad, que también necesitan evidencias, se suele utilizar registros, archivos de sistemas, diagrama de red, configuración de plataforma, etc.

Entrevistas

En el momento de realizar las entrevistas el auditor de certificación ISO 27001 sabe que la empresa utiliza la documentación necesaria, pero necesita conocer si todas las personas que se encuentran implicadas en el Sistema de Gestión de Seguridad de la Información se encuentran familiarizadas con dichos documentos y los utilizan para realizar todas las actividades.

Uno de los aspectos más importantes de la norma ISO 27001, no es la norma en sí, sino que los trabajadores de la empresa se encuentren concientizados. El auditor tiene que llevar a cabo entrevistas con todas las personas de la empresa para conocer el grado de conocimiento de los documentos más importantes del Sistema de Gestión de Seguridad de la Información. Estos pueden ser:

La política de seguridad de la información

Las cláusulas de confidencialidad

Utilizar los activos

La política de control de acceso

Las preguntas que se pueden realizar durante la entrevista son:

¿Tiene acceso a las normas internas de la organización que tengan relación con la seguridad de la información?

¿Me puede enseñar algunas de las políticas que se encuentran relacionadas?

¿Puede decir cuáles son los puntos más importantes de la política de seguridad?

El auditor se debe entrevistar con los responsables de los procesos, de los que podrá obtener la percepción de cómo se aplica la norma ISO 27001 en la empresa. Durante la realización de la entrevista las preguntan se dirigen para familiarizarse con las funciones y los roles que las personas tienen en el Sistema de Gestión de Seguridad de la Información y conocer si cumplen con todos los controles que sean implantado en la organización.

Cómo debe preparase

Como resumen se puede decir que un auditor que se encargue de la certificación bajo la norma ISO 27001 puede solicitar la siguiente información:

Los documentos requeridos para la norma ISO 27001 y cualquier documento que exista en un Sistema de Gestión de Seguridad de la Información.

Comprobar el cumplimiento de los documentos.

Realizar las entrevistas personales.

Si quiere estar preparado para las preguntas que el auditor que certifica un Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001 pueda realizar, lo primero que debe hacer es comprobar que se disponen de todos los documentos que pueden ser requeridos y después comprobar que la empresa hace todo lo que dice en los documentos y puede ser probado. Es importante que los trabajadores conozcan todos los documentos que son aplicables. Se tiene que asegurar que su empresa implementó de forma eficaz la norma ISO 27001 y acepta las operaciones que tiene que realizar cada día, ya que si no realiza esto se puede pensar que la documentación ha sido generada para satisfacer el auditor de certificación según la norma ISO 27001.

Las certificaciones aseguran que los productos y servicios son conformes a las expectativas de los clientes. En el caso de la seguridad de la información, la certificación ISO 27001 asegura a sus clientes el uso de buenas prácticas en materia de seguridad. Estas prácticas garantizan la confidencialidad, integridad, disponibilidad y legalidad de toda la información que gestionamos.

La norma ISO establece buenas prácticas que luchan contra los riesgos y las amenazas.

Qué supone una ISO 27001

Un análisis de riesgos, de todo tipo, no solo aspectos técnicos sino también físicos, organizativos y legales

La elaboración de procedimientos,

Varias auditorías internas y externas.

Su revisión periódica

Su actualización continúa

Su mejora

De esta forma, se asegura la actualización del sistema ante nuevas amenazas.

10. DESARROLLAR EL PLAN DE RECUPERACIÓN DESASTRES BASADOS EN EL ESTÁNDAR ISO 27001

1.0.1QUE ES UN PLAN DE CONTINGENCIA

El principal objetivo que tiene la ISO 27001 es asegurar que la empresa tiene la suficiente capacidad como para cubrir la demanda actual y futura de su negocio.

Se debe realizar un plan de capacidad, que incluirá todas las necesidades del negocio:

Los requisitos de rendimiento actual y futuro.

Planificar de forma temporal todos los costes que tendrán las actualizaciones.

Evaluar de forma anticipada todos los efectos que se generan en la capacidad de actualizar el servicio.

Prevenir los impactos que generan cambios externos, como pueden ser legislativos.

Los datos y procesos pueden realizar análisis predictivos.

Plan de contingencia

Un plan de contingencia en un Sistema de Gestión de Seguridad de la Información ISO-27001 se puede definir como: “presentación para tomar decisiones específicas cuando surja una condición que no se encuentre considerada en el proceso de planeación formal”.

Por lo que es un conjunto de procedimientos que permiten la recuperación en casos de desastres, un plan formal que describe todos los pasos que se tienen que seguir en caso de que suceda una emergencia.

Tiene diferentes fases que son:

Antes (como un plan de respaldo)

Durante (plan de emergencia)

Después (plan de recuperación tras el desastre)

Según la norma ISO 27001 establecer un adecuado plan de contingencia minimiza las pérdidas en caso de desastre y facilita la reanudación de las operaciones de una forma rápida, eficaz y oportuna.

El término desastre lo podemos definir como: “Interrupción en la capacidad de acceso a la información y el procesamiento de ésta mediante equipos informáticos, necesaria para el correcto funcionamiento del negocio”.

El plan de contingencia en un Sistema de Gestión de Seguridad de la Información es un control preventivo, ya que se establece como un instrumento que facilita la prevención eventual ante un desastre.

Es muy recomendable establecer un modelo del cual partan las organizaciones que se han preocupado por su desarrollo y crecimiento, que han establecido una estructura en la empresa con una función que define la administración de riegos, con lo que se obtienen grandes resultados.

El plan de contingencia implica que se debe invertir tiempo, dinero y esfuerzo, pero su valor sólo se puede medir en caso de que suceda algún desastre.

El principal objetivo que sigue el plan de contingencia en el SGSI ISO27001 es el de mantener la compañía y las actividades operando aún en una situación de desastre, por lo que se puede habilitar una opción en la que la empresa pueda dar una respuesta rápida a los problemas críticos, por lo que se permite una pronta recuperación de la operación normal en la organización.

El plan de contingencia depende mucho de la organización, ya que de forma inevitable supondrá unos elevados gastos. Aunque por otro lado, es muy importante conocer su utilidad ya que no depende de la probabilidad de que suceda un desastre, sino de las consecuencias que éste puede tener.

Se deben considerar todas pérdidas parciales o totales en los procesamientos de datos, y pueden venir causadas por:

Pérdidas financieras directas

Pérdidas financieras indirectas

Pérdidas en la producción

Pérdida de clientes

Incremento de costos en apoyo

Incremento de costos en compensación

Pérdidas de control

Obtener información incorrecta

Bases de datos pérdidas

En una organización, el plan de contingencia debe tener en cuenta dos aspectos básicos:

Operacional:

Cada usuario debe saber cuándo aparece un problema y debe saber a quién tiene que llamar. El plan de contingencia debe contener a las personas encargadas de tomar decisiones si sucede un desastre.

Administrativo:

Se contemplas aspectos como, definir los riesgos y los porcentajes, identificar las aplicaciones críticas, proceder a la recuperación de la información, especificar las alternativas, localizar los medios de respaldo, bases de datos que deben ser reconstruidos, localizar un software de reemplazo, localizar otro equipo de apoyo, obtener ayuda por parte de algún proveedor, generar un procedimiento que cuente con los pasos que se deben seguir durante el desastre y hasta que se vuelva a la normalidad, etc.

El plan de recuperación, según ISO-27001, debe tener las siguientes características:

Actual

Factible

Entendible

Documentado

Probado

1.0.2 DIFERENCIAS ENTRE BCP Y DRP

Actualmente, todas las organizaciones dependen de su sistema informático por lo que el más mínimo desastre o fallo en los sistemas puede ser fatal para la actividad de la misma, No es de extrañar que numerosas empresas de todos los tamaños pongan en práctica un plan de continuidad del negocio BCP o un plan de recuperación ante desastres DRP. Estos dos términos tienen cada uno sus propias particularidades y responden a objetivos bien distintos.

El BCP está orientado a garantizar la disponibilidad de las actividades más importantes de la empresa, define y pone en marcha un conjunto de procedimientos, arquitecturas y recursos con el fin de evitar tales interrupciones. Su principal misión es asegurar la disponibilidad continua de las infraestructuras informáticas como las redes, los centros de datos, los servidores y el almacenamiento, el BCP garantiza a los usuarios un servicio informático sin interrupciones. Además, un BCP generalmente se divide en dos componentes, el PCI (Plan de Continuidad Informático, orientado al sistema de información) y el PCO (Plan de Continuidad Operacional, orientado a la actividad de la empresa).

En cambio el DRP está orientado a la reconstrucción de la infraestructura informática y las aplicaciones estratégicas de la empresa. El DRP utiliza un plan de copias de seguridad que garantiza en caso de siniestro o incidente, la puesta en funcionamiento de la empresa, lo que reduce las consecuencias financieras. En función de las necesidades y del presupuesto de una empresa, un DRP se basa en numerosas estrategias que permiten recobrar la actividad en el menor tiempo posible. Es por ello, que la puesta en servicio de un DRP se determina en función de las probabilidades de riesgo, sus efectos y de la eficacia de los servicios involucrados. Entre las medidas que pueden definirse en el marco de un DRP se encuentran las copias de seguridad y los sistemas redundantes.

¿Por qué un backup online es esencial en un DRP?

El plan de recuperación ante desastres es un sistema muy completo para los posibles desastres informáticos. Los desastres naturales, los errores de manipulación, los fallos en el hardware y los virus representan verdaderas amenazas para los sistemas informáticos. Es por ello que la elaboración de un DRP debe incluir un backup online con el que asegurar la salvaguarda de los ficheros pues la multiplicación de riesgos obliga a las empresas a utilizar herramientas capaces de prevenir problemas informáticos y de gestionarlos cuando suceden. Las copias de seguridad permiten proteger la información pero según un estudio reciente, sólo el 27% de las PYMES interrogadas piensan que las medidas empleadas son suficientes. Cerca de la mitad admiten haber perdido parte de su información y el 70% de ellas han sido incapaces de recuperarla. Muchas empresas nunca han probado el backup antes de necesitarlo y algunas de ellas se quejan de la lentitud del mismo, obligándolas a interrumpirlo.

1.0.3 DESARROLLO Y ACTIVACIÓN DEL DRP

La recuperación de desastres se está convirtiendo en un aspecto cada vez más importante de la informática empresarial.

Como los dispositivos, sistemas y redes se vuelven cada vez más complejos, simplemente hay más cosas que pueden salir mal. Como consecuencia de ello, los planes de recuperación se han vuelto más complejos.

Un desastre podría ser el resultado de un daño importante a una parte de las operaciones, la pérdida total de una instalación

Ante la creciente dependencia de las empresas a los datos y el incremento de la complejidad en la infraestructura de TI, la importancia de contar con un DRP crece proporcionalmente.

Política de continuidad del negocio

Un punto de partida puede ser el desarrollo de una política encargada de establecer el marco de operación de los planes, así como la clasificación de los sistemas o aplicaciones para identificar aquellos que sean considerados como críticos.

Realizar una evaluación de riesgos

Una evaluación de riesgos permite identificar, analizar y evaluar las amenazas que podrían afectar a la organización, especialmente aquellos que puedan provocar un evento que se incluya en la categoría de desastre.

Realizar un análisis de impacto al negocio (BIA)

En este paso se definen principalmente los objetivos de recuperación para los sistemas que soportan los procesos de negocio. Se define el Tiempo Objetivo de Recuperación (RTO por sus siglas en inglés), que es el período permitido para la recuperación de una función o recurso de negocio a un nivel aceptable luego de un desastre, y el Punto Objetivo de Recuperación (RPO) que describe la antigüedad máxima de los datos para su restauración, con base en los requisitos del negocio.

Desarrollar estrategias de recuperación y continuidad del negocio

En este paso se busca dejar en claro todas las medidas a poner en práctica para regresar a la operación tan pronto como sea posible, con base en una priorización derivada de la clasificación del primer punto.

Concientizar, capacitar y probar los planes

Un elemento necesario con relación a los planes consiste en realizar su difusión entre los miembros de la organización, especialmente entre aquellos que serán los encargados de ponerlo en ejecución en caso de ser requerido. Además, es necesario que se lleven a cabo pruebas del mismo, para ello, se puede hacer uso de diferentes opciones, desde una revisión de la lista de verificación (checklist) de la recuperación hasta una prueba de interrupción completa (full interruption test) donde las operaciones se interrumpen en el sitio primario y se transfieren a un sitio de recuperación.

Mantener y mejorar el plan de recuperación ante desastres

A partir de los resultados de la prueba de los planes se deben llevar los ajustes correspondientes para contar con documentación actualizada y apropiada a los intereses de la organización, una vez que han sido consideradas las situaciones de desastre que podrían afectarla, las actividades y recursos necesarias para restablecer las operaciones críticas.

De manera general, las organizaciones que desarrollan los planes de recuperación deberán considerar los recursos a su alcance, los servicios previamente identificados y que se desean recuperar tan pronto como sea posible, así como los tipos y severidad de las amenazas que enfrenta la organización y pueden llegar a convertirse en un problema de mayor magnitud para la misma.

1.0.4 DESARROLLAR UNA POLÍTICA DE CONTINUIDAD DEL NEGOCIO

El Objetivo de una política de continuidad es Asegurar el desarrollo, la implementación y la revisión del sistema de gestión de la continuidad del negocio.

La política debe ser conocida por todo el personal que labora o presta sus servicios de forma directa o indirecta.

POLÍTICAS GENERALES.

1. El apego y conocimiento del Plan de Continuidad de Negocio es de carácter obligatorio, por todo colaborador.

2. La Dirección General es la única facultada para declarar o finalizar una contingencia, con excepción de cuando sea delegada esta facultad por escrito.

3 El área de Recursos Humanos, es responsable de la difusión del Plan de Continuidad de Negocio (BCP) a todo colaborador, con el fin de que sepan cómo actuar en caso de presentarse una contingencia.

4 Todo colaborador debe conocer si pertenece o no a un Servicio Critico.

5 Cada responsable de un Servicio Critico, debe proporcionar la capacitación adecuada para que sus colaboradores conozcan cómo deben actuar ante una contingencia

6 Es responsabilidad del departamento de Sistemas, mantener actualizados, disponibles, habilitados y configurados los equipos y sistemas necesarios en cada sitio alterno

. 7. Se definen como responsable de la ejecución del Plan de Continuidad de Negocio al jefe de Sistemas quien deberá comunicar la declaratoria de contingencia, coordinar y mantener informados a los responsables de los servicios críticos y a la Dirección General así como de comunicar la finalización de la contingencia.

8. Al término de una contingencia el responsable de cada Servicio Critico deberá realizar un informe del impacto que tuvo durante la misma, este deberá entregarse máximo al día hábil siguiente al jefe de sistemas.

9. Por su parte el área de Sistemas, elaborará su propio informe de la contingencia, contando con un máximo de un día hábil, posterior a la finalización de la contingencia para su entrega

10. Los reportes deberán remitirse a la Dirección General quien lo dará a conocer en el caso de una Auditoria.

11. El resultado de cada simulacro o prueba debe ser documentado y avalado por los responsables de los Servicios Críticos, y deben ser notificados a la Dirección

. POLÍTICAS PARTICULARES

. 1. RESPONSABILIDADES DE LA DIRECCIÓN GENERAL.

•Definir el alcance del Plan de Continuidad de la institución con relación a los procesos críticos así como sus limitaciones y exclusiones

. • Asegurar la disponibilidad de los recursos necesarios para cumplir los objetivos de continuidad estipulados, definiendo roles específicos por área crítica.

• Comunicar la importancia de que el Plan de Continuidad de Negocio (BCP) se implemente.

.MANTENIMIENTO DEL PLAN DE CONTINUIDAD.

1. el departamento de Sistemas es la responsable de elaborar, implementar y mantener actualizado las Estrategias de Continuidad de Negocio para los Servicios Críticos de la organización, en coordinación con los responsables de cada área así como de todos los documentos relacionados al Plan de Continuidad de Negocio

.2.Las actualizaciones al Plan de Continuidad de Negocio, se deberán realizar cuando se presente las siguientes condiciones:

• Se registren cambios en los Servicios Críticos.

• Existan cambios en la legislación aplicable.

• Existan cambios importantes en la estrategia y responsabilidades de Negocio.

• Después de la implementación de un nuevo proceso de negocio y que se considere crítico

• Posterior al resultado de una prueba o simulacro o bien una contingencia o desastre real.

• Cambios en la estructura organizacional relacionados a los Servicios Críticos (se consideran cambios en los colaboradores y cambios en la dependencia del área que provee los Servicios Críticos)

. 3. La finalidad de la prueba o simulacros es identificar los puntos vulnerables y proporcionar experiencia sobre la ejecución al personal que lo lleve a cabo. Esta actividad debe realizarse al menos de forma anual o antes si se presenta un cambio importante al Plan de Continuidad de Negocio. Ante una actualización del Plan de Continuidad de Negocio, el alcance de la prueba o simulacro podrá ser parcial de

Acuerdo al cambio realizado y esta deberá ejecutarse dentro de los siguientes 90 días.

4. Con cada actualización del Plan de Continuidad de Negocio, los responsables de los Servicios Críticos deben garantizar la capacitación de los colaboradores involucrados

. CAPACITACIÓN.

1 La campaña se debe realizar en los siguientes escenarios:

• El curso de inducción debe contener un apartado relacionado al Plan de Continuidad de Negocio, informando al colaborador de nuevo ingreso si se integra a un área de Servicio Critico.

• Todo colaborador reconocerá el Plan de Continuidad de Negocio, como parte de la vida y cultura organizacional.

• Cuando se asignen nuevos integrantes a los grupos de recuperación.

• Cuando se dé una reorganización de la Organización.

• Deber realizarse una capacitación periódica anual a todos los empleados

• Cuando exista una actualización del Plan de Continuidad de Negocio

DE LOS SIMULACROS O PRUEBAS

. El alcance del simulacro será definido por la Dirección General, indicando Servicios críticos y escenarios a probar

. Debe calendarizarse la ejecución de pruebas o simulacros, considerando lo previsto en el apartado Mantenimiento del Plan de Continuidad de Negocio

, y estas fechas deben ser del conocimiento de las áreas consideradas con Servicios Críticos.

Los responsables de los Servicios Críticos, deben colaborar en las pruebas o simulacros y tomar las debidas consideraciones para no afectar los niveles de servicio.

. SANCIONES. La infracción a las normas contenidas en este documento traerá como consecuencia, según la gravedad del caso, la imposición de las sanciones previstas en el Reglamento Interno de Trabajo y, de ser necesario, las establecidas en las leyes que sean aplicables.

11 IMPLEMENTAR LOS PROCESOS DE SEGURIDAD INFORMÁTICA

1.1.1 IMPORTANCIA DE LA IMPLEMENTACIÓN DEL MANUAL DE POLÍTICAS DE SEGURIDAD

El departamento de servicios educativos necesita realizar la implementación de las políticas de seguridad, ya que son un conjunto de instrucciones y directrices, que sirven como guía para los empleados, donde se establecen criterios de seguridad que deben ser acogidos por cada uno de los integrantes de la institución.

.

Una vez implementadas y en funcionamiento las políticas de seguridad Informática, cada empleado tendrá claro lo que debe hacer al estar dentro de la institución, protegiendo a la misma de forma general, sabiendo la importancia de la información que depende de cada uno de ellos, aprovechando de la mejor manera los recursos tecnológicos de los cuales se disponen.

Todos y cada uno de los empleados que laboran en la institución deben ser involucrados tanto en el desarrollo de las mismas así como capacitándolos.

Mantener capacitados a los empleados así como tener las políticas Correctamente implementadas, es muy importante para prevenir nuevos ataques, manteniéndose así en un mejor nivel de seguridad.

Se plantea un documento que se encuentra anexo como Manual de Políticas de Seguridad Informática, que recoge las políticas de seguridad informática necesarias para la entidad, que incluye las siguientes políticas:

Política general de seguridad de la información

Política de seguridad de accesos

Política de seguridad de operaciones

Política de continuidad de negocio

Política de recuperación de desastres

Infracciones a las políticas de seguridad

1.1.2 LINEAMIENTOS GENERALES DE SEGURIDAD DE LA INFORMACIÓN

La dirección y el departamento de servicios educativos, deben declarar que conoce y aplicará cada una de las políticas y procedimientos establecidos para el uso de la misma, aceptando las responsabilidades por el uso que se le dé a esta.

Solamente las autoridades debidamente autorizados, identificados y autentificados, tendrán acceso al sistema operativo y a los sistemas de información, limitados por los roles establecidos de acuerdo a sus funciones y responsabilidades.

El Área de Sistemas mantiene una separación lógica de las redes para la navegación: acceso a la red institucional e Internet para los trabajadores y acceso internet WIFI para los visitantes.

El Área de Sistemas estará facultada para filtrar páginas web, de tal modo que se controle el contenido servido y el ancho de banda utilizado. También podrá revisar de forma periódica el historial de navegación.

La navegación está regida por los principios de control, seguridad y uso racional, controlándose a través de políticas de navegación a través de un proxy.

1.1.3. PRUEBAS DE SEGURIDAD DE POLÍTICAS

Será necesario realizar algunas pruebas al personal de la institución una vez que ya hayan sido capacitados y concientizados para saber que llevan a la práctica las medidas de seguridad informática implementadas en la institución por ejemplo una prueba sencilla seria una encuesta al personal para saber su grado de conocimiento. Estas mismas encuestas revelarán si es necesario algún ajuste por si ha surgido algún hecho que se haya dejado de lado, o al programa de concientización, por si los empleados desconocen de ellas.

Tabla 11. Pruebas a Políticas de Seguridad Informática a empleados

Departamento de servicios educativo del colegio nacional de educación PRUEBAS A POLITICAS DE SEGURIDAD INFORMÁTICA				
Fecha:		Hora:		Consecutivo:
Dependencia:				
Empleado:				
Núm.	Aspecto a evaluar	Si	No	Observaciones
1	¿Conoce las funciones que debe desempeñar en su puesto de trabajo?			
2	¿La entidad cuenta con políticas de seguridad informática?			

3	¿Conoce las políticas? (Mencione al menos 2)			
4	¿Ha recibido capacitación respecto a las políticas de seguridad?			
5	¿Maneja o tiene a su cargo activos			

informáticos? (Mencione cuales son)				
6	¿Tiene acceso a internet desde su computadora?			
7	¿Almacena información confidencial en su computadora?			
8	¿Comparte esta información por algún medio sin cifrarla?			
9	Realiza periódicamente Copias De Seguridad (Back Up) De La Información (Indicar la periodicidad y dónde la hace)			
10	¿Tiene cuenta de correo electrónico institucional? (Indicar su cuenta)			

11	¿Conoce la clave de acceso a su correo electrónico? (Indicar su suministrar su clave			Esta pregunta para verificar si pueden clave) fácilmente
12	¿Posee clave para acceso al equipo de trabajo?			
13	¿Cambia de forma periódica las claves de acceso al equipo y/o al correo?			

También se pueden realizar pruebas a la página web de la institución en busca de posibles fallos de seguridad como malware en el servidor, así como también un test de penetración y además, se verifica que el proxy esté bloqueando sitios prohibidos en el departamento y en general a la institución.

Una vez que se termina el análisis, la web muestra un resumen de las pruebas realizadas y las detecciones obtenidas, para el caso en particular, se observa que la página está limpia de virus o infecciones

Otro herramienta para detectar malware es la Página web de Sucuri la cual la podemos encontrar tecleando https://sitecheck.sucuri.net/

Al igual que estas pruebas se podrían realizar técnicas usuales en la evaluación de la vulnerabilidad de un sistema las cuales pueden ser: Network scanning, Port scanning, Password cracking (identificación de contraseñas “débiles”), revisión de logs, chequeo de la integridad (checksums, hash, firmas digitales), detección de virus, escaneo de conexiones wifi no autorizadas, o el test de penetración.

Las pruebas son para detectar las vulnerabilidades que una vez implementadas las políticas de seguridad informática deberían ser nulas o mínimas al momento de realizarlas:

En general se realizan pruebas de:

Vulnerabilidad administrativa. Defectos en políticas, procedimientos o actividades de seguridad.

Vulnerabilidad física. Defectos físicos, geográficos, de personal o en los controles relacionados.

Vulnerabilidad técnica. Defectos en los controles lógicos de los sistemas de la organización (routers mal configurados, puertas traseras en los programas, contraseñas débiles,…)

La implantación de un sistema de gestión de vulnerabilidades implica que éstas han sido identificadas, se ha determinado como tratar cada una de ellas y las acciones tomadas han sido monitorizadas y trazadas. Como resultado de esta gestión de vulnerabilidades hemos de tener:

Priorización de los sistemas.

Priorización de las vulnerabilidades.

Definición de roles y responsabilidades respecto a la gestión de vulnerabilidades.

Identificación, para cada software y tecnología, de fuentes relevantes de información sobre identificación de vulnerabilidades

Análisis de riesgos para incorporar o no un parche o actualización relacionado con una vulnerabilidad y para decidir los pasos a realizar, que puede incluir la realización de pruebas para evaluar que no hay efectos adversos sobre otros sistemas.

Se permite, en circunstancias especiales o de emergencia, la instalación de parches o actualizaciones siguiendo un proceso de respuesta a incidentes.

Se permite llevar a cabo acciones provisionales (cambio de accesos o privilegios, p.ej.) o controles alternativos, mientras no pueda incorporarse un parche que cubra la vulnerabilidad.

Registro de la actividad (audit log) en relación con la gestión de vulnerabilidades.

Revisión y monitorización periódica del proceso de gestión de vulnerabilidades.

Cumplimiento de bloqueo a sitios web prohibidos.

El ingreso a sitios web que no brinden ningún beneficio al trabajador en sus labores diarias, sino que por el contrario sirve de distracción, fueron bloqueados por el administrador de la red, conforme a las políticas implementadas de seguridad informática basadas en ISO 27001.

Fue necesario instalar un Proxy en la red usando el software Squid, para que todas las conexiones pasaran a través de este y así poder filtrar lo estrictamente permitido. Dos de las páginas bloqueadas son: www.facebook.com y www.youtube.com, debido al alto grado tanto de distracción como de consumo del ancho de banda.

Como herramienta para la generación de reportes de los datos que pasan por el proxy Squid, se instaló el software SARG:

Con SARG, se obtienen diversos reportes, dentro de los cuales se encuentra el acceso a sitios por usuario, y el de sitios bloqueados

Podemos por medio de la ip del dispositivo que se conecta a internet quien realizo realizó varios intentos de ingresar a www.facebook.com y a www.youtube.com y páginas web que se encuentran bloqueadas.

Y en el reporte de sitios denegados, se muestran las direcciones IP de los usuarios, así como la fecha y hora del intento de ingreso a uno de los sitios web bloqueados.

12 CAPACITAR AL PERSONAL ACTIVO EN LA EJECUCIÓN DE LOS PROCESOS DE SEGURIDAD

1.2.1 LA IMPORTANCIA DE CAPACITAR Y CONCIENTIZAR A LOS EMPLEADOS

Una vez que el manual de políticas de seguridad informática resultado de este proyecto para el departamento del plantel ha sido aprobado por la dirección general de esta institución, es necesario realizar el plan de divulgación y concientización de las mismas, con el fin de que los trabajadores las conozcan, sepan utilizarlas y de esta forma interioricen conceptos de seguridad informática y buenas prácticas para proteger la información de la entidad.

El propósito general de la concientización del usuario es el de enfocar cada uno de los trabajadores en las políticas de seguridad informática, estableciendo así los comportamientos a reforzar, como por ejemplo: no dejar contraseñas escritas en papeles, elaborar de forma periódica una copia de seguridad, mantener el escritorio limpio, etc., además de esto, darles a entender que la seguridad de los activos informáticos no sólo depende de los especialistas en el tema, sino que cada uno de ellos hacen parte de ello y que son piezas fundamentales en la protección de la información.

Un punto que se debe dejar muy claro en las capacitaciones que se realicen, son los procesos disciplinarios para los usuarios que no tienen sentido de pertenencia hacia la entidad y no cumplen con las políticas. Estos procesos serán diseñados por la dirección general.

De igual forma, se recomienda establecer incentivos, ya sean por áreas o de forma personal, premiando de esta forma a los trabajadores que se encuentren comprometidos con el desarrollo y crecimiento de las políticas de seguridad, ya que así se incentiva y motiva al trabajador, cambiando para bien las costumbres con las que vienen laborando desde hace muchos años.

Al igual que el manual de las políticas de seguridad, la entidad debe aprobar y destinar recursos para el desarrollo del programa de concientización.

1.2.2 CÓMO DESARROLLAR UN PROGRAMA DE CAPACITACIÓN

El programa de sensibilización en seguridad de la información tiene como metas principales

1) Comunicar formalmente a toda la entidad la existencia del subsistema de gestión de seguridad de la información y sus componentes de apoyo

2) Socializar a todo el personal de la Entidad las políticas de seguridad de la información

3) Socializar los principales procedimientos de seguridad de la información

4) Fomentar la cultura de la seguridad de la información como herramienta de protección de la información institucional

5) Explicar de manera sencilla las normas legales que soportan el sistema de gestión de seguridad de la información

6) Divulgar a todo el personal los principales riesgos de seguridad de la información

7) Explicar de manera sencilla en qué consisten diversos tipos de ataques informáticos y como controlarlos

8) Explicar los mecanismos de control dispuestos por la entidad para evitar ataques informáticos

Todos los trabajadores se beneficiaran con este proyecto al obtener un conocimiento adecuado de cómo manejar con seguridad su información en distintos dispositivos además de contextualizarse de las regulaciones que tiene la institución para darle apoyo.

Temáticas del plan de sensibilización

Conocimiento general del Subsistema de gestión de seguridad Se cubrirán conocimientos fundamentales de la seguridad de la información: Concepto de seguridad de la información

- Qué es un riesgo de seguridad de la información.
- Qué es la norma ISO27001 de gestión de seguridad de la información
- Cómo está estructurado el sistema de gestión de seguridad de la información
- Quienes son los actores del sistema de gestión de seguridad de la información
- Conocimiento de las políticas de seguridad de la información
- Explicación de la política general de la seguridad de la información
- Explicación de las políticas de seguridad de la información con ejemplos de aplicación
- Conocimiento de los procedimientos principales del Subsistema de gestión de seguridad
- Explicación del procedimiento de clasificación y etiquetado de información
- Explicación del procedimiento de Acceso a áreas seguras
- Metodología de gestión de riesgos para identificación de riesgos de seguridad Amenazas informáticas Phishing Ransomware Robo de identidad
- Generalidades sobre regulación en materia de seguridad de la información Ley de trasparencia y acceso a la información
- Ley de protección de datos personales

- Mensajes de correos electrónico
- Publicaciones en pantallas
- Elementos físicos de recordatorios
- Materiales y recursos mensajes electrónicos sobre que debe y que no debe hacerse.
- videowalls o pantallas institucionales.
- Screensavers con mensajes de sensibilización.
- Elementos de oficina con mensajes alusivos.
- Eventos relacionados con seguridad (concursos, dramatizaciones)
- Evaluación, Mejora y Seguimiento
- La campaña se evaluará mediante encuesta electrónica en donde los colaboradores calificaran las diferentes actividades, su impacto y utilidad para el desarrollo de sus funciones asignadas.

.

1.2.3 ASPECTOS IMPORTANTES EN CONCIENCIACIÓN EN SEGURIDAD DE LA INFORMACIÓN

ISO 27001 es implementada para mantener a salvo la información de cualquier entidad empresarial, organización o institución cualquier pérdida o extravío de la misma puede causar un mal funcionamiento en la entidad.

Por eso es que es muy importante que los colaboradores de la entidad se concienticen, Si ellos no toman conciencia de la importancia de la información que pasa por sus manos difícilmente ésta será protegida correctamente.

Podemosmencionar3 aspectos claves para que la concientización en Seguridad de la Información en el personal funcione:

Demostrar convincentemente que las brechas de seguridad no solo afectan negativamente a la organización, sino que también puede dañar a los empleados de manera individual.

Se debe enfocar y reforzar constantemente los fundamentos de una fuerte práctica de seguridad.

Debe ser atractiva para los empleados haciendo hincapié en la importancia que tiene para ellos.

¿Cómo se podría lograr ese objetivo? Se pueden seguir ciertas instrucciones que, aplicadas a cada caso, darán buenos resultados en la institución:

Capacitar a los empleados para reconocer comportamientos de falta de seguridad en sí mismos y en los demás.

Realizar una buena gestión del programa de concienciación sobre Seguridad de la Información e ISO-27001. La dirección general debe entender la seguridad y apoyar las iniciativas de sensibilización.

Involucrar a los empleados en la creación de objetivos de seguridad y comprobar que todos entienden lo que la falta de la misma puede provocar.

Educar e informar sobre seguridad.

Asegurarse que tanto empleados como directivos conocen que hay una cadena de seguridad, cada uno tiene un papel y unas funciones a la hora de afrontar problemas y ponerles solución.

Fomentar discusiones en mesa redonda sobre seguridad de la información y el Sistema de Gestión de ISO27001, en la que discutir sobre los riesgos de la información de la empresa.

CONCLUSION

Al finalizar este proyecto la seguridad de la información que posee el departamento de servicios educativos y en general el plantel aumentará de forma notoria al tener elaborado e implementado un manual por cual puedan regirse para contrarrestar los riesgos a los cuales se encuentran expuestos, el cual será una referencia continua para la utilización correcta de los recursos informáticos con los que cuentan en esa institución educativa

El análisis de riesgo que se realizó obtuvo una visión global de las vulnerabilidades a las que se estaba expuesto, resaltando algunos fallos existentes en la seguridad informática. Es muy recomendable actualizarlo de manera periódica para mantener al margen nuevas amenazas que puedan surgir de manera futura, por la continua actualización en los sistemas de información.

Las políticas de seguridad informática fueron desarrolladas e implementadas en base a la norma de estandarización ISO 27001 la cual consiste en la creación de un Sistema de Gestión de Seguridad Informática; para las buenas prácticas del

manejo de la información, mostrando los dominios y controles para cada uno de ellos, siendo el primero, Política de Seguridad Informática.

Se recomienda que una vez aprobado el documento de Políticas de Seguridad Informática se coloque en marcha su implementación, estableciendo cronogramas de capacitación para sus empleados y mitigar de esta forma los riesgos a los cuales se encuentran expuestos.

Una vez se realice la implementación, es necesario efectuar pruebas para verificar el cumplimiento de cada una de las políticas utilizando al menos el formato de encuestas creados en este proyecto

La realización de este proyecto es el primer paso para la implementación de un Sistema de Gestión de Seguridad Informática en la entidad, y de esta manera se podrá lograr una mejora continua en la gestión de la seguridad, garantizando además una continuidad y disponibilidad de las operaciones de la entidad, y por consiguiente la reducción de los costos que pudieran surgir por una imprevisto informático.

Anexos A

MANUAL DE POLÍTICAS DE SEGURIDAD INFORMÁTICA

MANUAL DE POLÍTICAS DE SEGURIDAD INFORMÁTICA

Información del documento

Versión	Fecha	Elaborado por	Razón de la actualización
1	05/04/2020	Israel Guarneros Moreno	Creación del documento

CONTENIDO

POLÍTICAS DE SEGURIDAD INFORMATICA BASADAS EN ISO 27001

INTRODUCCIÓN

En la actualidad es necesario mantener un control de los activos informáticos y de información debido a los ataques cibernéticos que puede sufrir una red computacional en una institución es por ello que es necesario minimizar los problemas que puedan presentarse en los bienes y llevadas a cabo de manera correcta por todo el personal de la institución.

El documento presentado servirá como herramienta para cada una de las autoridades de la institución para su aplicación y estricto cumplimiento, concientizando a todo el personal en el uso correcto de todos los activos sensibles de la información (equipos, sistemas operativos, sistemas de información y los datos en general) así como sus debilidades y fallas para que sean resueltas en caso de presentarse

.

ALCANCE

Las políticas basadas en ISO 27001 que en este documento se plasman son de carácter obligatorio para todos los directivos, coordinadores y jefes que hagan uso directa o indirectamente de tecnologías de información y comunicaciones.

COMPROMISO DE LA DIRECCIÓN

La dirección aprueba las políticas contenidas en este documento, así como también su apoyo en:

El fomento de manera activa para la creación de una cultura de seguridad dentro de la entidad.

Divulgación de estas políticas a cada uno de los trabajadores de la institución.

Supervisar que las políticas del presente manual se cumplan.

ACTUALIZACIÓN

Por las consideraciones establecidas en este documento, se revisará por lo menos una vez cada seis (6) meses para actualizarlo y/o agregar nuevas políticas que permitan el adecuado uso de las tecnologías de información y los sistemas operativos en el Conalep Ing.Bernanrdo Quintana

LINEAMIENTOS DE POLÍTICAS

Toda la información que se encuentre en los equipos de cómputo , será de carácter confidencial, por lo que ningún trabajador podrá hacer uso de ella con fines personales, tampoco podrá facilitarla a personal externo en cualquier forma de transmisión.

Los equipos designados a cada trabajador serán de su uso exclusivo y con fines laborales, siendo responsable de los daños realizados al mismo o al sistema operativo.

POLÍTICAS DE SEGURIDAD

1.- Disposición y Manejo de los Equipos de Cómputo

Se asignará a quien así lo necesite por su trabajo una computadora para apoyar al cumplimiento de sus labores.

Estos equipos son activos de la institución.

Cada usuario es responsable del equipo quese le asigne, por lo que es responsable de su cuidado.

No se permite el traslado de los equipos de cómputo o sus partes a un área distinta a la que fue asignado. Para poder realizarlo se debe solicitar por escrito al Jefe del Área de Sistemas

Solo el personal del Área de Sistemas está facultado para abrir, desarmar, cambiar o instalar piezas del equipo de cómputo, así como formatear, instalar, reinstalar o modificar el sistema operativo o cualquier otro programa en la estación de trabajo.

No es permitido el uso de dispositivos de almacenamiento extraíbles como memorias USB o discos externos.

Los equipos deben estar conectados correctamente en los tomas de corriente regulada.

Evitar la exposición directa al sol o al polvo.

No está permitido fumar así como tampoco el consumo de alimentos y/o bebidas en los puestos de trabajo.

Informar de forma oportuna cualquier incidente que impida el buen funcionamiento del equipo y/o del sistema operativo al Área de Sistemas (Formato Reporte de Incidente).

Las solicitudes de instalación o cambio, ya sea del equipo completo o alguna de sus partes, deben ser aprobadas por los jefes del área solicitante y del Área de Sistemas.

2. Recursos compartidos

La institución asignará a cada usuario una cuenta para el ingreso a la red de datos, con la cual podrán acceder a una carpeta personal así como otra para compartir archivos con los demás usuarios. Para el correcto uso y funcionamiento, se establecen las siguientes políticas:

Deben ser utilizados solo por personal de la institución

Los directorios asignados deben utilizarse sólo para fines institucionales, evitando guardar archivos personales además de fotos, música, videos o material innecesario.

Realizar una copia de seguridad de la información vital para el área de trabajo, al menos una vez al mes por cada usuario (Máximo 50MB por usuario).

Evitar acceder, modificar o borrar información privada de otros usuarios ajenos a su propiedad.

Los archivos y carpetas almacenados en la red son propiedad de la institución, sin que exista un derecho particular sobre ellos.

3. Cuentas de Usuario

Los trabajadores que requieran de cuentas institucionales deberán estar identificados para acceder al sistema operativo y al sistema de información mediante una cuenta de usuario, la cual tendrá ciertos permisos o privilegios dependiendo del rol asignado. Para este ítem se aplicarán las siguientes políticas:

Toda solicitud de creación de cuenta o modificación de la misma debe realizarse por escrito (Jefe del Área Administrativa), debidamente autorizada por los jefes del área solicitante y del Área de Sistemas.

Sólo el Jefe del Área de Sistemas podrá eliminar una cuenta de usuario.

El Jefe del Área Administrativa, deberá informar de manera oportuna situaciones que impliquen creación, modificación y/o borrado de cuentas de usuario, tales como rotación de personal, despidos o renuncias, etc., con el fin de mantener la base de datos de usuarios actualizada.

No se crearán cuentas de Invitado, tampoco a personal externo.

4. Contraseñas de Usuario

Se verifica que el usuario que intenta ingresar al sistema sea quien dice ser, mediante un mecanismo de autenticación, compuesto por la combinación de usuario y contraseña.

La contraseña es un conjunto de caracteres que cada funcionario debe entregar al sistema operativo y a la aplicación de la entidad para poder hacer uso del equipo, debe contener caracteres en minúsculas y mayúsculas, números y al menos un carácter especial, completando un mínimo de ocho (8) caracteres, siendo así robusta y difícil adivinar por terceros.

El usuario y la contraseña deben ser de uso personal.

Queda prohibido imprimir, escribir o mostrar la combinación de usuario y contraseña.

Se limitará a 3 intentos de acceso, después de éstos, se suspenderá por quince (15) minutos la cuenta.

5. Uso de Internet

Se permitirá el acceso a internet a los trabajadores, de acuerdo a las siguientes políticas:

Se utilizará solamente para fines laborales, evitando de esta forma saturar el ancho de banda, haciendo buen uso del servicio.

Queda prohibido el ingreso a redes sociales, páginas de entretenimiento, pornografía, violencia o cualquier otra ajena a las funciones diarias.

Queda prohibida la descarga de material ilícito o de contenido con derechos de autor.

No está permitida instalación de software que utilice el ancho de banda para acceder o descargar cualquier contenido, o para realizar llamadas nacionales o internacionales.

6. Correo Electrónico

Sólo se permitirán usuarios permanentes de la institución.

Toda comunicación debe ser de carácter laboral.

Queda prohibido iniciar o responder cadenas de correo electrónico de cualquier tipo.

Los usuarios deben ser precavidos al abrir mensajes de personas desconocidas, evitando abrir archivos adjuntos que puedan afectar el software instalado en el equipo.

Evitar el envío de correos de forma masiva, enviando los mensajes sólo a personas estrictamente necesarias.

Se limita el tamaño de envío y recepción de mensajes a 5MB de información adjunta.

No facilitar el usuario y la contraseña a terceras personas.

Queda prohibido el envío de correos con material ilícito, contenido sexual o violento.

7. Administración de Servidores

En relación a los servidores y el Área de Sistemas, se establecen las siguientes políticas:

El área de los servidores, debe permanecer con acceso restringido, sólo el personal autorizado tiene permitido el ingreso.

Cualquier persona externa que ingrese a la Oficina de Sistemas, debe registrarse en la bitácora de ingreso, proporcionando su nombre, firma y motivo de ingreso.

Queda prohibida la manipulación de los equipos del área de servidores por personal no autorizado para ello.

Un conjunto de copias de seguridad de la información de los servidores debe ser trasladado a otros sitios seguros.

Todos los equipos deben estar conectados a un sistema de alimentación ininterrumpida de corriente eléctrica.

El cuarto de servidores debe estar en la temperatura adecuada, manteniendo un segundo aire acondicionado de respaldo.

8. Del uso e instalación del software en los equipos de cómputo

El Área de Sistemas será la encargada de determinar de acuerdo con las necesidades particulares de los funcionarios cual es el software a instalar en los equipos de cómputo.

Solo el Área de Sistemas puede realizar instalaciones, modificaciones de software y de las configuraciones del mismo en los equipos de cómputo.

Solo se tendrá instalado software que este licenciado y que sea de carácter legal.

Se podrá instalar software tipo Free, GNU, Shareware, Demos partiendo de un análisis de licenciamiento, seguridad, y de una necesidad particular solicitada expresamente por el usuario o cualquier persona autorizada mediante carta dirigida al jefe del Área de Sistemas y que lo considere necesario para el desarrollo de sus funciones administrativas.

9. Seguridad del Personal

El Jefe de la División Administrativa, debe asegurar antes de la realización de una contratación las responsabilidades de seguridad, describiendo de forma clara y

precisa el cargo, así como los términos y condiciones del contrato, el cual debe incluir una cláusula de confiabilidad y cumplimiento de las políticas de seguridad del presente documento.

El Jefe de la División Administrativa debe validar que la información suministrada por los aspirantes a algún cargo disponible sea verás, antes de que su vinculación definitiva.

El Jefe de la División Administrativa, debe desarrollar un programa de concientización sobre protección de la información para todo el personal.

Todo el personal deberá asistir a los cursos que se impartan dentro del programa de concientización, aplicando los conocimientos adquiridos en sus puestos de trabajo.

Cuando se dé porfinalizado un contrato, el personal saliente debe firmar un acuerdo de confidencialidad para evitar la fuga de información sensible o clasificada como reservada.

10 CONTINUIDAD DEL NEGOCIO

El Objetivo de una política de continuidad es Asegurar el desarrollo, la implementación y la revisión del sistema de gestión de la continuidad del negocio.

La política debe ser conocida por todo el personal que labora o presta sus servicios , de forma directa o indirecta.

.

El apego y conocimiento del Plan de Continuidad de Negocio es de carácter obligatorio, por todo colaborador.

La Dirección General es la única facultada para declarar o finalizar una contingencia, con excepción de cuando sea delegada esta facultad por escrito.

El área de Recursos Humanos, es responsable de la difusión del Plan de Continuidad de Negocio (BCP) a todo colaborador, con el fin de que sepan cómo actuar en caso de presentarse una contingencia.

Todo colaborador debe conocer si pertenece o no a un Servicio Critico. En consecuencia sí pertenece a un servicio crítico, debe conocer su línea de comunicación (Participante). La relación de Participantes y colaborador de un servicio crítico se encuentran definidos en los documentos “Estructura de respuesta y finalización de incidentes” y en “Estrategias de Continuidad de Negocio”.

Cada responsable de un Servicio Critico, debe proporcionar la capacitación adecuada para que sus colaboradores conozcan cómo deben actuar ante una contingencia

Es responsabilidad del departamento de Sistemas TI, mantener actualizados, disponibles, habilitados y configurados los equipos y sistemas necesarios en cada sitio alterno

.Se definen como responsable de la ejecución del Plan de Continuidad de Negocio al jefe de Sistemas TI quien deberá comunicar la declaratoria de contingencia, coordinar y mantener informados a los responsables de los servicios críticos y a la Dirección General así como de comunicar la finalización de la contingencia.

.Al término de una contingencia el responsable de cada Servicio Critico deberá realizar un informe del impacto que tuvo durante la misma, este deberá entregarse

máximo al día hábil siguiente, una vez finalizada la contingencia. Se deberá utilizar el formato “Afectación de Servicio Critico” y marcar copia al jefe de Sistemas TI.

Por su parte el área de Sistemas TI elaborará su propio informe de la contingencia utilizando el formato “Reporte Post Mortem de Afectación al Servicio”, contando con un máximo de un día hábil, posterior a la finalización de la contingencia para su entrega

Los reportes de “Afectación de Servicio Critico” y “Post Mortem de Afectación al Servicio”, deberán remitirse a la Dirección General quienes los darán a conocer en el caso de una Auditoria.

El resultado de cada simulacro o prueba debe ser documentado y avalado por los responsables de los Servicios Críticos, y deben ser notificados a la Dirección

11 Otras Políticas

Existen algunas políticas de seguridad que no están establecidas en los apartados anteriores; por lo que se establecerán a continuación:

No se brindará soporte técnico a equipos personales sin excepción debido a que no son propiedad de la entidad.

No deben ser cambiadas ninguna de las configuraciones del sistema operativo, como por ejemplo, las direcciones IPs.

No utilizar el espacio en disco de los equipos con archivos que no sean necesarios para el desarrollo de sus funciones.

Todos los trabajadores con equipos de cómputo a su cargo deben apagar completamente los equipos al finalizar su jornada laboral con el fin de ahorrar energía eléctrica

12 - Generalidades

Todo el personal de la institución, está obligado a reportar cualquier vulnerabilidad, riesgo o inconveniente presentado, con el fin de evaluarlos y seguir ajustando el presente documento y los planes de contingencia dispuestos para los equipos de cómputo y el sistema operativo en cada uno de ellos. Por lo anterior, el personal del Área de Sistemas debe mantener un sentido ético y responsable de la información recibida de carácter personal y/o confidencial

13- infracciones y Sanciones

Todo el personal de la entidad queda sujeto al cumplimiento de las normas aquí expuestas, so pena de ser sancionado disciplinaria y/o legalmente, si hubiera lugar a ellas. Las sanciones van desde un llamado de atención hasta la suspensión del cargo, dependiendo de la gravedad de la falta cometida, además de la malicia o perversidad con que se cometa.

Las acciones que se enumeran a continuación, constituyen infracciones a la Política de Seguridad.

1. Son acciones de falta u omisión a las Políticas Generales de Seguridad de la Información:

a) No firmar los acuerdos de confidencialidad o de responsabilidad de activos de información.

b) No actualizar la información de los activos de información a su cargo.

c) No reportar los incidentes de seguridad o las violaciones a las políticas de seguridad, cuando se tenga conocimiento de ellos.

d) No guardar de forma segura la información cuando se ausente de su puesto de trabajo o al terminar la jornada laboral.

e) Dejar información en carpetas compartidas, no autorizadas o en lugares distintos al servidor de archivos institucional, obviando las medidas de seguridad.

f) Dejar las gavetas abiertas o con las llaves puestas en los escritorios.

g) Permitir que personas ajenas a la Institución, deambulen sin acompañamiento en el interior de las instalaciones, en áreas no destinadas al público.

h) Solicitar cambio de contraseña de otro usuario.

i) No realizar el borrado seguro de la información en equipos o dispositivos de almacenamiento, para traslado, reasignación o para disposición final.

j) Utilizar claves de acceso de un usuario distinto al propio para ingresar a los sistemas y/o aplicativos.

2. Son acciones de mal uso de la plataforma tecnológica institucional:

a) Hacer uso de la red de datos institucional, para acceder, almacenar, mantener o difundir en o desde los equipos institucionales, material con contenido sexual u ofensivo, cadenas de correos y correos masivos no autorizados.

b) La utilización de software no relacionado con la actividad laboral que pueda degradar el desempeño de la plataforma tecnológica institucional.

c) Actuar con negligencia en el cuidado de los equipos, dispositivos portátiles o móviles entregados para actividades propias de la institucion

d) Conectar equipos de cómputo personal u otros sistemas electrónicos personales a la red de datos institucional, sin la debida autorización.

e) El utilizar los recursos tecnológicos institucionales para beneficio personal.

f) Instalar programas o software no autorizados en las estaciones de trabajo o equipos portátiles institucionales, cuyo uso no esté autorizado por la Dirección de Tecnologías de la Información y Comunicaciones.

3. Son acciones de sabotaje de la plataforma tecnológica institucional:

a) Impedir u obstaculizar el funcionamiento a los aplicativos, bases de datos o a las redes de telecomunicaciones y datos, sin estar autorizado.

b) Destruir, dañar, borrar, deteriorar activos informáticos, sin autorización.

c) Distribuir, enviar, introducir software malicioso u otros programas de computación de efectos dañinos en la plataforma tecnológica de la institucion

d) Alterar datos personales de las bases de datos institucionales.

e) Realizar cambios no autorizados en la plataforma tecnológica.

4. Son acciones de acceso no autorizado a la infraestructura tecnológica de la institución:

a) Accedersin autorizaciónexpresaa todooen partealossistemasde la institución.

b) Suplantar a un usuario ante los sistemas de autenticación y autorización establecidos.

c) No mantener la confidencialidad de las contraseñas de acceso a la red de datos, los recursos tecnológicos o los sistemas de información o permitir que otras personas accedan con el usuario y clave del titular a éstos.

d) Otorgar el acceso o privilegios a la infraestructura a personas no autorizadas.

e) Ingresar a carpetas sin autorización.

5. Son acciones de robo de información:

a) Ejecutar acciones tendientes a eludir o variar los controles establecidos por la institucion

b) Retirar de las instalaciones de la Institución, estaciones de trabajo o equipos portátiles que contengan información institucional, sin la autorización pertinente.

c) Sustraer de las instalaciones documentos con información institucional, o abandonarlos en lugares públicos o de fácil acceso.

d) Entregar, enseñar y divulgar información institucional, a personas o entidades no autorizadas.

e) Copiar sin autorización programas o violar los derechos de autor o acuerdos de licenciamiento.

ANEXO B FORMATO DE INVENTARIO


Inventario de activos sensibles de información

Compañía:

Valor Actual del Inventario

Fecha

Equipo	Responsable	Departamento	Sucursal	Categoría	Descripción	Marca	Modelo	Serial Nº	Nº de identificación del equipo

REFERENCIAS

Lourdes Munch (2021) calidad y mejora continua principios de calidad y certificación ISO. México. Trillas

Jorge Ramio Aguirre, Josemaría MiretBiosca. (2006). Seguridad Informática y Criptografía. España: RA-MA Editorial

Martha Irene Romero Castro Grace Liliana Figueroa Morán Denisse Soraya Vera Navarrete José Efraín Álava Cruzatty Galo Roberto Parrales Anzures Christian José Álava Mero Ángel Leonardo Murillo Quimiz Miriam Adriana Castillo Merino. (2018). INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES. Ecuador: Editorial Área de Innovación y Desarrollo, S.L

Farias-Elinos, Ma. C, Mendoza-Díaz & L. Gómez-Velazco. (Farias-Elinos, Ma. C, Mendoza-Díaz & L. Gómez-Velazco). “Las Políticas de Seguridad como Apoyo a la Falta de Legislación Informática. México: McGraw-Hill.

María Gabriela Hernández Pinto, Bertha Alice Naranjo Sánchez... (2006). DISEÑO DE UN PLAN ESTRATÉGICO DE SEGURIDAD DE INFORMACIÓN EN UNA EMPRESA México: Mc. Graw Hill.

Dussan Clavijo, Ciro Antonio. (2016). Políticas de seguridad informática. Cali, Colombia: Universidad Libre.

Rodríguez Nelly Ethel, Horacio Villa García. (2009). Seguridad Informática para alumnos de la Escuela Secundaria. . México: McGraw-Hill

Felipe Bracho Carpizo, José Roberto Sánchez Soledad. (2018). el valor de la privacidad: datos personales en tiempos del panóptico. Seguridad cultura de prevención para ti, 31, 59

Álvaro Gómez vélites. (2015). enciclopedia de la seguridad informática. México: alfa omega

Hugo scolnik. (2011). una mirada a la seguridad informática. Serie de conocimiento, 12, 142

Gonzalo Álvarez Marañón. (2017). a mi lista de deseos seguridad informática para la empresa y particulares. México: McGraw-Hill.

Jorge Domínguez Chávez. (2015). Seguridad Informática Personal y Corporativa. México: IEASS, Editores.

Silvia M. Quiroz-Zambrano, David G. Macías-Valencia. (2017). Seguridad en informática: consideraciones. México: Alfaro.

Daniel Felipe González Agudelo. (2014). EL RIESGO Y LA FALTA DE POLITICAS DE SEGURIDAD INFORMÁTICA UNA AMENAZA EN LAS EMPRESAS CERTIFICADAS. México: Edomex

Maíllo Fernández, Juan Andrés. (2017). Seguridad Digital E Informática. México: rama

JuanVoutssasM.*.(2010). Preservacióndocumentaldigital yseguridad informática. Investigación bibliotecológica, 24, 125.

Boquera, M (2003). Servicios avanzados de telecomunicaciones. Ediciones Díaz de Santos. España. Bugarini, F (2010). Una propuesta de seguridad de la información. Obtenida el 02 de enero del 2014

López, D (2009). Análisis inicial de la anatomía de un ataque a un sistema informático. Recuperado el 06 de abril de 2014.

http://www.seguinfo.com.ar/tesis/anatomia_ataque_sistema_informatico.zip
Mcleod, J (2000).

Ministerio de Ciencia e Innovación. Orden de Comité de Seguridad de la información. Recuperado el 15 de marzo de 2014, de http://www.mineco.gob.es/stfls/mineco/ministerio/ficheros/Orden_CSI_firmada.

Ripoll, J (2012). Seguridad en los Sistemas Informáticos (SSI). Recuperado el 15 de abril de 2014, de http://www.segu-info.com.ar/tesis/

Rojas Soriano, R (2002). Investigación social: teoría y praxis. Editorial Plaza y Valdés. México

Solís Salazar, C. (2014). ¿Qué son las Políticas de Seguridad de la Información? Recuperado el 28 de marzo de 2014, de http://www.solis.com.ve/que-son-las-politicas-de-seguridad-de-la-informacion.

Stallings, W (2004). Fundamentos en seguridad de redes .Prentice Hall. España.

Monzón, I., Prendes, R., Falcón, P., Diéguez, M. (2004). “Implantación de los Sistemas de Gestión de Calidad ISO 27001”. CIGUET Cienfuegos. Recuperado de: http://www.monografias.com/trabajos27/implantacion-sistemas/implantacionsistemas.shtml#sistemas#ixzz4BxUqmhFw

ISO (2016). ISO/IEC 27000:2016 Preview. Information technology -- Security techniques -- Information security management systems - Overview and vocabulary. Ginebra: International Organization for Standardization.

Joyanes, L. (2010). Introducción: estado del arte de la ciberseguridad. En "Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio", 13-46. Cuadernos de estrategia, 147. España: Ministerio de Defensa.

Leiva, E. (2015). Estrategias Nacionales de Ciberseguridad: Estudio Comparativo Basado en Enfoque Top-Down desde una Visión Global a una Visión Local. Revista Latinoamericana de Ingeniería de Software, 3(4), 161-176

Ochoa, P. (2015). Gobierno de Seguridad de la Información, un enfoque hacia el cumplimiento regulatorio. Revista Tecnológica ESPOL - RTE, 28(3), 1-17.

Paya, C.; Cremades, A. & Delgado, J. (2016). El fenómeno de la ciberdelincuencia en España: La propuesta de la Universidad de Nebrija en la capacitación de personal para la prevención y el tratamiento del ciberdelito.

Revista Policía y Seguridad Pública, 7(1), 237-270. DOI: http://dx.doi.org/10.5377/rpsp.v7i1.4312

Pons, V. (2017).

Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. URVIO, Revista Latinoamericana de Estudios de Seguridad, 20, 80-93. DOI: http://dx.doi.org/10.17141/urvio.20.2017.2563

Rodríguez, G. (2016). Ciberseguridad realidad y tendencias en Venezuela. Cuestiones Jurídicas, 10(1), 13-39.

Rodríguez P., 2016). ¿Qué seguridad? Riesgos y Amenazas de Internet en la Seguridad Humana. Araucaria. Revista Iberoamericana de Filosofía, Política y Humanidades, 18(36), 391-415. DOI: http://dx.doi.org/10.12795/araucaria.2016.i36.17

Salon, J. (2010). El ciberespacio y el crimen organizado. En "Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio", 131-164. Cuadernos de estrategia, 147. España: Ministerio de Defensa.

Vallés, L. (2016). La ciberseguridad en el mundo actual. TINO, 50, 585-620.

Vargas, R.; Recalde, I. & Reyes, R. (2016). Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa. URVIO.

Luis Gómez y Pedro Pablo Fernández Rivero. (2019). Como implantar un SGSI según ISO/IEC 27001 y su aplicación en el esquema nacional de seguridad. COLOMBIA: ALFAOMEGA

Alberto Alexander. (2007). seguridad de información. México: alfa omega.

Cristina Merino Bada, Ricardo Cañizares Sales. (2011). Implantación de un Sistema de Gestión de seguridad de la Información según ISO 27001: Un enfoque práctico. España: fceditorial

BORGHELLO, Cristian. Segu.Info. Políticas de Seguridad de la Información. [En línea]. <http://www.segu-info.com.ar/politicas/polseginf.htm>. [Citado en 4 de Diciembre de 2014].

COLOMBIA. MINISTERIO SALUD Y LA PROTECCIÓN SOCIAL. Resolución 1995 de 1999 (8, Julio, 1999). Por la cual se establecen normas para el manejo de la Historia Clínica. Bogotá: El Ministerio, 1999. 8 p.

CRISTIANSE, Eric. Concientización en Seguridad de la Información. [En línea]. <http://www.cybsec.com/upload/Molinos_Jornada_Cybsec_Eric_Cristianse.pdf> [Citado en 10 de Mayo de 2015].

GUÍA DE SEGURIDAD DE LAS TIC [En línea]. <https://www.ccn-cert.cni.es/publico/herramientas/pilar44/en/help/manual_usuario_pilar_basic-4.3.pdf> [Citado en 17 de Abril de 2015].

LOBO PARRA, Leonard David y OVALLOS, Jesús Andrés y SIERRA GÓMEZ, Ana María. Plan de gestión de la seguridad de la información de la Biblioteca Argemiro Bayona de la Universidad Francisco de Paula Santander Ocaña, mediante la aplicación de la norma ISO 27001 y técnicas de ethical hacking. Ocaña, 2012, 33 h. Trabajo de grado (Especialista en Auditoría De Sistemas). Universidad Francisco De Paula Santander Ocaña, Facultad de Ingeniería.

MAGERIT Seguridad Informatica. [En línea]. <http://seguridadinformaticaufps.wikispaces.com/MAGERIT> [Citado en 19 de Abril de 2015].

MAGERIT – versión 3.0 Libro I - Método [En línea]. <http://administracionelectronica.gob.es/ctt/resources/7e6c82fb-9607-43e3-a70b-080a27a02bf7?idIniciativa=184&idElemento=85> [Citado en 17 de Abril de 2015].

MAGERIT – versión 3.0 Libro II - Catálogo de Elementos [En línea]. <http://administracionelectronica.gob.es/ctt/resources/a9fff834-15f6-499b-ae5f-ff7b9989ddc5?idIniciativa=184&idElemento=86> [Citado en 17 de Abril de 2015].

MAGERIT – versión 3.0 Libro III - Guía de Técnicas [En línea]. <http://administracionelectronica.gob.es/ctt/resources/01e54e9c-bf49-4b85-aa40-e3dccbcb13d3?idIniciativa=184&idElemento=87> [Citado en 17 de Abril de 2015].

MIFSUD, Elvira. Monográfico: Introducción a la seguridad informática - Políticas de seguridad. En: Observatorio Tecnológico del Gobierno de España. [En línea]. <http://recursostic.educacion.es/observatorio/web/ca/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=4> [Citado en 3 de Diciembre de 2014].

PERAFÁN RUIZ, John Jairo y CAICEDO CUCHIMBA, Mildred. Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor Del Cauca. Popayán, 2014, 132 h.

PILAR EAR / [En línea]. <http://www.pilar-tools.com/es/tools/pilar/v53/help_es/cia/index.html> [Citado en 18 de Abril de 2015].

ROMO VILLAFUERTE, Daniel y VALEREZA CONSTANTE, Joffre. Análisis e implementación de la norma ISO 27002 para el departamento de Sistemas de la Universidad Politécnica Salesiana sede Guayaquil. Guayaquil, Ecuador, 2012, 183

.

SÁNCHEZ, Esteban. Análisis y gestión de riesgos en la UPCT con PILAR [En línea]. <http://www.rediris.es/difusion/eventos/foros-seguridad/fs2012/archivo/analisis_riesgos_upct.pdf> [Citado en 17 de Abril de 2015]

.

SECURITY ART WORK. Análisis de riesgos con PILAR (II). [En línea]. <http://www.securityartwork.es/2012/11/13/analisis-de-riesgos-con-pilar-ii/> [Citado en 18 de Abril de 2015].

SUÁREZ SIERRA, Lorena. Sistema de Gestión de la Seguridad de la Información. Bogotá: Universidad Nacional Abierta y a Distancia UNAD, 2013.

VILLAMIZAR R, Carlos. Jugando a crear cultura de seguridad de la información – De la teoría a la práctica. [En línea]. <http://www.magazcitum.com.mx/?p=2361#.VXHGhM9_Oko> [Citado en 10 de Mayo de 2015].

Solís Salazar, C. (2014). ¿Qué son las Políticas de Seguridad de la Información? Recuperado el 28 de marzo de 2014, de http://www.solis.com.ve/que-son-las-politicas-de-seguridad-de-la-informacion

Ripoll, J (2012). Seguridad en los Sistemas Informáticos (SSI). Recuperado el 15 de abril de 2014, de http://www.segu-info.com.ar

Cappuccio, V (2006). Políticas de Seguridad. Recuperado el 06 de abril de 2014,http://www.monografias.com/trabajos11/seguin/seguin.shtml

Chávez, R (2013). Gestión de Riesgo de Seguridad de la Información. Recuperado el 06 de abril de 2014, http://www.slideshare.net/roberth.chavez/gestin-del-riesgos-de-seguridad-dela-informacin

ISMS Forum Spain. La importancia de contar con una política de seguridad en la empresa. Obtenida el 18 de febrero del 2014, de http://www.protegetuinformacion.com/perfil_tema.php?id_perfil=7&id_tema=6

Isocron Systems. La importancia de usar contraseñas seguras. Obtenida el 18 de febrero del 2014, de http://www.isocron.net/blog/2011/08/02/laimportancia-de-usar-contrasenas-seguras.

López, D (2009). Análisis inicial de la anatomía de un ataque a un sistema informático. Recuperado el 06 de abril de 2014, http://www.seguinfo.com.ar/tesis/anatomia_ataque_sistema_informatico.zip

Recasens, E (2009). Análisis de Riegos de un Sistema de Información. Recuperado el 06 de abril de 2014, http://www.segu-info.com.ar/tesis/gestionde-riesgos.zip

Vega, J (2009). Análisis de Riesgo y Seguridad de la Información. Recuperado el 05 de abril de 2014, http://www.segu-info.com.ar/tesis/gestionriesgo.zip

Bey non-Davies, P. (2015). Sistemas de información: introducción a la informática en las organizaciones. Barcelona, España: Editorial Reverte.

Cañón Parada, L. J. (2015). Ataques informáticos, Ética Hacking y conciencia de seguridad informática en niños. (Trabajo de Fin de Grado). Universidad Piloto, Colombia