INSTITUTO TECNOLOGICO SUPERIOR DE TANTOYUCA

ING. SISTEMAS COMPUTACIONALES

Administración de Redes.

DOCENTE:

Ing. Edgar Medellín Orta

ALUMNO(A):

Arely Alejandra de Jesús Rendon

"POLITICAS DE SEGURIDAD PARA UNA EMPRESA"

Contenido

I. INTRODUCCIÓN

La falta de políticas y procedimientos en seguridad es uno de los problemas más graves que confrontan las empresas hoy día en lo que se refiere a la protección de sus activos de información frente a peligros externos e internos.

Las políticas de seguridad son esencialmente orientaciones e instrucciones que indican cómo manejar los asuntos de seguridad y forman la base de un plan maestro para la implantación efectiva de medidas de protección tales como: identificación y control de acceso, respaldo de datos, planes de contingencia y detección de intrusos, entre otros.

Dichas las políticas varían considerablemente según el tipo de organización de que se trate, en general incluyen declaraciones generales sobre metas, objetivos, comportamiento y responsabilidades de los empleados en relación a las violaciones de seguridad. A menudo las políticas van acompañadas de normas, instrucciones y procedimientos, deberán definir las áreas sobre las cuales debe enfocarse la atención en lo que concierne a la seguridad.

En el presente documento se engloban algunas de las políticas de seguridad que notablemente deben de implementarse en una empresa sin importar el concepto para el cual se desempeñen, esto con la finalidad de que sean de beneficio en todos los puntos posibles para la compañía misma.

II. OBJETIVOS

OBJETIVO GENERAL

Definir Políticas de Seguridad de las Tecnologías de la Información y las Comunicaciones en el Instituto, las cuales serán el fundamento para obtener un control efectivo sobre la información, su resguardo y las actividades de los funcionarios y empleados del Instituto que son realizadas a través de operaciones de cómputo o del uso de equipos y recursos informáticos, proveyendo la información necesaria que permita a todos los funcionarios, ejecutivo, empleados, participantes, beneficiarios del sistema y otros actores asociados al instituto, crear conciencia de la necesidad de proteger la Información, el Hardware, el Software para el mejor manejo de las redes de datos y comunicaciones.

OBJETIVOS ESPECIFICOS

- Integración de la seguridad como tema estratégico y concientización global sobre la importancia de la seguridad de la información.
- Planeamiento y manejo de la seguridad más efectivos.
- Mayor seguridad en el ambiente informático, minimizar los riesgos inherentes a la seguridad de la información
- Generar una mejor y oportuna reacción a incidentes de seguridad.
- Orden en la elaboración de tareas y responsabilidades de cada funcionario bajo las normas que facilitaran la comunicación entre los mismos.
- Mayor facilidad para la toma de decisiones.
- Mejora de la imagen institucional.
- Mejora del ambiente laboral.
- Mayor control de la información recibida y/o proporcionada a terceros y aumento de la confianza de los mismos.

III. ALCANCE

Las presentes Políticas de Seguridad, son aplicables a la administración de:

Información: Datos ordenados, clasificados y almacenados en cualquier medio (magnético, papel, correo electrónico, conversación telefónica, chat, usb, etc.).

Software: Conjunto de Sistemas Operacionales, programas, productos y aplicaciones que utiliza el INSTITUTO.

Hardware: Conjunto de equipos de cómputo, telecomunicaciones y redes que utiliza el INSTITUTO.

IV. DEFINICIONES

Archivos: Conjunto de datos o instrucciones que se almacenan en el Disco Duro y/o cualquier otro medio de almacenamiento con un nombre que los identifica.

Autorización: Proceso o procedimiento oficial del INJUPEMP por el cual el usuario autenticado recibe los permisos para efectuar acciones sobre elementos del sistema de información.

CPU: (Unidad Central de Proceso): Es una parte del Hardware o equipo de cómputo que realiza el procesamiento de datos.

Contraseña: Password o clave para obtener acceso a un programa o partes de un programa determinado, una terminal u ordenador personal (computadora portátil o de escritorio), un punto en la red (fijo o inalámbrico), etc.

Contraseña Robusta: Password o clave que cumplen con las condiciones específicas de acuerdo a la normativa internacional para la seguridad de la información.

Encriptado: Cifrado o codificación de la información sensible que puede ser recibida o enviada desde o para los sistemas de información de la empresa.

Disco duro: Medio utilizado para el almacenamiento de información. Cuando se almacena información en un disco, ésta se conserva incluso después de apagar el computador y se encuentra guardada de forma permanente en el interior del Hardware.

Disponibilidad: Característica relacionada con la facilidad y oportunidad de acceso a la información cuando sea requerida por los procesos del instituto para realizar sus negocios ahora y en el futuro.
Equipos de cómputo: Son los dispositivos eléctricos, electrónicos y mecánicos que se emplean para procesar o consultar, transmitir, almacenar datos. (Hardware)

Hacker: Término utilizado para llamar a una persona con grandes conocimientos en informática y telecomunicaciones y que los utiliza con un determinado objetivo. Este objetivo puede o no ser maligno o ilegal. La acción de usar sus conocimientos se denomina hacking o hackeo. Popularmente se le

conoce como piratas informáticos a aquellos hackers que realizan acciones malignas con sus conocimientos.

Hardware: Partes físicas de un sistema de procesamiento de datos, por ejemplo, la CPU, el monitor, la impresora, teclado, ratón, módems, teléfonos, enrutador, switches, etc.

Incidente: Es todo evento que surge a raíz de una definición inadecuada del alcance de un producto, mala práctica en el sistema, operación o una violación a las Políticas de Seguridad de la Información y que conlleva a una falla en la operatividad normal dentro del Instituto.

Información: conjunto de datos sobre un suceso o fenómeno en particular que al ser ordenados en un contexto sirven para disminuir la incertidumbre y aumentar el conocimiento sobre un tema específico. Es todo lo que puede ser expresado a través de un lenguaje y es utilizada por el instituto durante el desarrollo de sus operaciones.

Información Sensible: Información que por su naturaleza debe mantenerse bajo estrictas medidas de seguridad que garanticen el acceso sólo al personal autorizado y para un propósito previamente definido.

Información Interna: Es aquella información de uso interno que utilizan los empleados de la compañía con el propósito de realizar las operaciones normales del instituto. Son ejemplos de información interna: los registros o datos obtenidos o generados de los participantes.

Información Pública: Todo archivo, registro, dato o comunicación contenida en cualquier medio, documento, registro impreso, óptico o electrónico u otro que no haya sido clasificado como reservado y que está disponible para la distribución pública por medio de los canales autorizados, en congruencia con las disposiciones que establece la Ley de Transparencia y Acceso a la Información Pública.

Integridad: Es el mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados, así como su validez de acuerdo con los requerimientos del instituto.

Monitor: (pantalla): Permite visualizar electrónicamente la salida de datos de un computador.

Parche de Seguridad: Conjunto de instrucciones de corrección para un software en especial, que sirven para solucionar sus posibles carencias, vulnerabilidades, o defectos de funcionamiento, en el Código original de este.

Programas (software): Conjunto de instrucciones que permiten manejar una tarea en procesamiento electrónico de datos, por ejemplo: office, módulo financiero, módulo de planillas, registro de afiliación, correo corporativo, chat corporativo, etc.

Protector de pantalla: Imagen o diseño móvil que aparece en la pantalla cuando transcurre un determinado período de tiempo durante el que no se mueve el ratón (Mouse) o se presiona una tecla. Los protectores de pantalla evitan que la pantalla resulte dañada como consecuencia de la presentación de áreas oscuras y luminosas en la misma posición durante largo tiempo.

Recursos informáticos: Software, hardware y redes que posee y/o utiliza la compañía.

Riesgo de la Información: Es una combinación de la posibilidad de que una amenaza contra un activo de información ocurra aprovechando una vulnerabilidad y/o falla en un control interno, y la severidad del impacto adverso resultante.

Sistema: Conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso, generados para cubrir una necesidad u objetivo.

Vulnerabilidad: Debilidad de un sistema, que da posibilidad de realizar alguna acción que afecte negativamente a éste.

V. NORMATIVA Y ESTANDARES APLICABLES RELACIONADOS

Las presentes Políticas de Seguridad están desarrolladas con base en estándares sobre Sistemas de Gestión de la Seguridad de la Información (SGSI), disposiciones vigentes que son aplicables, tales como:

- ISO/IEC 27000 - vocabulario estándar para el SGSI. Quinta versión: febrero 2018. ISO/IEC 27000:2018.
- ISO / IEC 27001: 2013 - requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información dentro del contexto de la organización.

VI. RESPONSABLES

Las presentes Normas y Políticas de Seguridad de la Información son aplicables a todas las áreas, departamentos, secciones o entidades de la empresa y son de cumplimiento obligatorio por parte de todos los funcionarios y empleados del Instituto en cualquier nivel jerárquico, sean temporales o permanentes, definidos como los usuarios y administradores de la información y equipos informáticos, así como por otros usuarios que utilicen de una u otra forma los sistemas de información o las redes tecnológicas.

Comité de Seguridad Informática.

Está compuesto por los representantes de los distintos departamentos de la Compañía, así como por el Gerente de Informática, el Gerente de Telecomunicaciones (cuando exista), y el abogado o representante legal de la Compañía. Este Comité está encargado de elaborar y actualizar las políticas, normas, pautas y procedimientos relativas a seguridad en informática y telecomunicaciones. También es responsable de coordinar el análisis de riesgos, planes de contingencia y prevención de desastres. Durante sus reuniones, el Comité efectuará la evaluación y revisión de la situación de la Compañía en cuanto a seguridad informática, incluyendo el análisis de incidentes ocurridos y que afecten la seguridad.

Gerencia de Informática

Es responsable de implantar y velar por el cumplimento de las políticas, normas, pautas, y procedimientos de seguridad a lo largo de toda la organización, todo esto en coordinación con la Junta Directiva y la Gerencia de Telecomunicaciones (cuando exista). También es responsable de evaluar, adquirir e implantar productos de seguridad informática, y realizar las demás actividades necesarias para garantizar un ambiente informático seguro. Además, debe ocuparse de proporcionar apoyo técnico y administrativo en todos los asuntos relacionados con la seguridad, y en particular en los casos de infección de virus, penetración de hackers, fraudes y otros percances.

Jefe de Seguridad

Es responsable de dirigir las investigaciones sobre incidentes y problemas relacionados con la seguridad, así como recomendar las medidas pertinentes.

Administrador de Sistemas

Responsable de establecer los controles de acceso apropiados para cada usuario, supervisar el uso de los recursos informáticos, revisar las bitácoras de acceso y de llevar a cabo las tareas de seguridad relativas a los sistemas que administra, como, por ejemplo, aplicar inmediatamente los parches correctivos cuando le llegue la notificación del fabricante del producto o de un ente como el CERT (Computer Emergency Response Team). El Administrador de Sistemas también es responsable de informar al Jefe de Seguridad y a sus superiores sobre toda actividad sospechosa o evento insólito. Cuando no exista un Jefe de Seguridad, el Administrador de Sistemas realizará sus funciones.

Usuarios

Son responsables de cumplir con todas las políticas de la Compañía relativas a la seguridad informática y en particular:

- Conocer y aplicar las políticas y procedimientos apropiados en relación al manejo de la información y de los sistemas informáticos.
- No divulgar información confidencial de la Compañía a personas no autorizadas.
- No permitir y no facilitar el uso de los sistemas informáticos de la Compañía a personas no autorizadas.
- No utilizar los recursos informáticos (hardware, software o datos) y de telecomunicaciones (teléfono, fax) para otras actividades que no estén directamente relacionadas con el trabajo en la Compañía.
- Proteger meticulosamente su contraseña y evitar que sea vista por otros en forma inadvertida.
- Seleccionar una contraseña robusta que no tenga relación obvia con el usuario, sus familiares, el grupo de trabajo, y otras asociaciones parecidas.
- Reportar inmediatamente a su jefe inmediato a un funcionario de Seguridad Informática cualquier evento que pueda comprometer la seguridad de la Compañía y sus recursos informáticos, como por ejemplo contagio de virus, intrusos, modificación o pérdida de datos y otras actividades poco usuales.

El incumplimiento de las presentes Políticas de Seguridad dará lugar a la aplicación de las sanciones laborales establecidas de conformidad al Código de Trabajo, el Reglamento Interno de Trabajo de la compañía y demás disposiciones internas relacionadas, sin perjuicio de las acciones civiles o penales que, en su caso, puedan resultar aplicables.

VII POLITICAS DE SEGURIDAD

POLÍTICAS DE SEGURIDAD DE APLICACIÓN GENERAL

SEGURIDAD DE HARDWARE (EQUIPO COMPUTACIONAL PARA TRABAJO)

1. El Usuario es responsable de mantener el Hardware que le ha sido asignado debidamente identificado para efectos de control de inventario. El Área responsable (Departamento de Bienes) deberá mantener los registros de inventario debidamente actualizados.
2. Se prohíbe utilizar la Información, Hardware y Software, para realizar actividades diferentes a las estrictamente laborales.
3. Se prohíbe mover el Hardware, reubicarlo o llevarlo fuera del Instituto sin la autorización del titular de la Oficina que lo tiene asignado y la debida autorización escrita extendida por el departamento de Bienes y el traslado debe estar motivado por los intereses y objetivos de la compañía.
4. Está prohibido modificar la configuración de hardware y software establecida. Tampoco está permitido hacer copias del software para fines personales.
5. El Usuario debe realizar su debido respaldo (Backup) de la información que generar o utiliza en su equipo, en forma periódica.
6. Para prevenir el acceso no autorizado, los usuarios deben usar un sistema de contraseñas robusto y además deben configurar el protector de pantalla para que se active al cabo de 15 minutos de inactividad y que requiera una contraseña al reasumir la actividad. Además el usuario debe activar el protector de pantalla manualmente cada vez que se ausente de su oficina.
7. Es responsabilidad del Usuario evitar el deterioro del Hardware, para lo cual deberá cumplir las siguientes reglas básicas:
    - No ingerir ni dejar alimentos y/o bebidas cerca y/o encima del Hardware.
    - No colocar objetos pesados encima del Hardware.
    - Mantener alejado del Hardware cualquier elemento electromagnético como imanes, teléfonos, radios, etc.
    - No colocar el Hardware en lugares inestables y/o expuestos a ser golpeados involuntariamente o que estén en riesgo de caer y dañarse parcial o totalmente.

- No abrir el Hardware. De ser necesaria dicha labor será llevada a cabo por el Área de
- Soporte Técnico de la Unidad Técnica de Informática.
- Es responsabilidad de los Usuarios conservar siempre limpio su lugar de trabajo, así como su Hardware.
- Conservar los cables en buen estado, ordenados y correctamente conectados. No debe existir ningún tipo de tensión, evitando siempre el doblado de los mismos.

SEGURIDAD DE USUARIOS Y CONTRASEÑAS

1. Es responsabilidad del área encargada de la administración de usuarios, asignar un nombre único de usuario y es responsabilidad del usuario tener una contraseña robusta reservada en cada sistema informático, los cuales deberán ser confidenciales e intransferibles para garantizar su óptima identificación.
2. Ningún usuario o programa debe utilizar las contraseñas de administrador de sistemas, salvo personal autorizado.
3. Es responsabilidad del Usuario no guardar su contraseña en una forma legible en archivos en disco; tampoco debe escribirla en papel, dejarla en sitios donde pueda ser encontrada o compartirla o revelarla a cualquier otra persona.

POLÍTICAS DE SEGURIDAD DE APLICACIÓN ESPECÍFICA

AREA DE SISTEMAS.

SEGURIDAD DE SERVIDORES

1. Es responsabilidad del jefe de la Unidad Técnica de Informática de la empresa, asignar a todos los servidores internos instalados en el Instituto, un responsable por la administración del sistema de cada uno y contar como mínimo con la siguiente información relacionada:
   - Nombre del Servidor
   - Localización del Servidor
   - Nombre del administrador responsable y localización al igual que su suplente
   - Detalle especifico del Hardware
   - Sistema operativo y su versión
   - Aplicaciones y bases de datos
   - Función principal y/o uso

- Acuerdos de mantenimiento (Plan detallado – Cronograma)

2. Es responsabilidad de cada administrador del sistema, que todos los servidores, así como su sistema operativo, tengan estándares de configuración de seguridad documentados y aplicados de acuerdo al rol del servidor en la organización, así como mantenerlos con las actualizaciones más recientes de seguridad.
3. Es responsabilidad del Jefe de la Unidad Técnica de Informática, definir los procesos tecnológicos, mantenerlos actualizados y velar por su cumplimiento, para mantener los servidores protegidos físicamente en un ambiente con control de acceso y protección ambiental.

SEGURIDAD DE EQUIPOS DE COMUNICACIÓN

1. Las direcciones internas, configuraciones e información relacionada con el diseño de los sistemas de comunicación, video seguridad y cómputo deben ser tratadas como Información **Confidencial**.
2. Queda terminantemente prohibido que los empleados y funcionarios de la compañía lleven a cabo algún tipo de instalación de líneas telefónicas digitales o análogas, canales de transmisión de datos, módems o cambiar su configuración, esto es responsabilidad exclusiva del área de Informática o de cualquier empresa que se haya contratado para tal fin, en cuyo caso deberá ser supervisada por la Unidad Técnica de Informática.
3. Es responsabilidad del Asistente del Jefe de la Unidad Técnica de Informática (Jefe de Producción y Data Center), llevar control estricto y actualizado de la topología, archivos y parámetros de configuración de la red; así como el inventario de equipos y software de la misma esto con el fin de tener un control de los activos de infraestructura de la empresa.

SEGURIDAD EN CENTROS DE CÓMPUTO Y TELECOMUNICACIONES

1. Los Centros de Cómputo y Área de Telecomunicaciones de la empresa estarán clasificadas como áreas de acceso restringido solo para personal autorizado.
2. Es responsabilidad del Jefe de la Unidad Técnica de Informática, asegurar que todos los recursos de computación y Telecomunicaciones del Instituto, cuenten con planes de mantenimiento preventivo y/o correctivo debidamente contratados.
3. Los Centros de Cómputo y las áreas de telecomunicaciones del Instituto deberán contar con sistemas de control de acceso físico, que puedan ser auditados.

VIII. CONCLUSION

La finalidad de las políticas de seguridad que se describieron en el presente documento proporciona instrucciones específicas sobre cómo mantener más seguros tanto los computadores de la Compañía (conectados o no en red), como la información guardada en ellos. La violación de dichas políticas puede acarrear medidas disciplinarias e incluso el despido.

Este documento deberá estar en constante actualización para integración de nuevas políticas o en su caso mejoras, con el fin de sumar mayor protección y disminución del riesgo en la vulnerabilidad de la información de la empresa.

IX. REFERENCIAS BIBLIOGRAFICAS

El Blog Ceupe. (2019, 30 julio). POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y SGSI. Recuperado 3 de julio de 2020, de https://www.ceupe.com/blog/ejemplo-politica-seguridad-informacion-y-sgsi.html

C.Victor, C. (s. f.). Políticas de Seguridad. Recuperado 3 de julio de 2020, de https://www.monografias.com/trabajos11/seguin/seguin.shtml

Carisio, C. (s. f.). Políticas de seguridad informática y su aplicación en la empresa. Recuperado 3 de julio de 2020, de https://blog.mdcloud.es/politicas-de-seguridad-informatica-y-su-aplicacion-en-la-empresa/

INCIBE. (2019, 20 julio). ¿Por qué cifrar la información sensible? Recuperado 3 de julio de 2020, de https://www.incibe.es/protege-tu-empresa/blog/cifrar-informacion-sensible