INSTITUTO TECNOLOGICO SUPERIOR DE TANTOYUCA

ING. EN SISTEMAS COMPUTACIONALES

ASIGNATURA: ADMINISTRACION DE REDES

DOCENTE: ING.EDGAR GUILLERMO MEDELLIN ORTA

ACTIVIDAD COMPLEMENTARIA 1

NOMBRE DEL ESTUDIANTE:

OSIEL MARCIAL ANTONIO DOMÍNGUEZ

GRUPO: S8A

FECHA: 22/06/2020

INDICE

INTRODUCCION

La información y los recursos informáticos son activos importantes y vitales, por lo que las máximas autoridades y todos los empleados en cualquier nivel jerárquico, tienen el deber de custodiarlos, preservarlos, utilizarlos y mejorarlos. Esto implica que se deben tomar las acciones pertinentes para asegurar que la información y los sistemas informáticos estén apropiadamente protegidos contra muchas clases de amenazas y riesgos, por lo que deben adoptarse y aplicarse medidas de seguridad.

POLITICAS DE SEGURIDAD

Seguridad de información

- Se debe asegurar que la información no este expuesta o revelada a personas no autorizadas
- Se debe asegurar consistencia de los datos prevenir la creación, alteración o borrado de datos de entidades no autorizadas

Seguridad de hardware y software.

- Se prohíbe utilizar la Información, Hardware y Software, para realizar actividades diferentes a las estrictamente laborales
- Está prohibido modificar la configuración de hardware y software establecida por la Unidad Técnica de Informática. Tampoco está permitido hacer copias del software para fines personales.

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.
- 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.

De infraestructura de telecomunicaciones y de instalaciones

- Se prohíbe tener como herramientas de trabajo, computadores portátiles (laptops), CPU's, USB´s o cualquier otro equipo de propiedad del usuario, salvo autorización previa emitida por el jefe de mayor jerarquía del área que corresponda
- Es responsabilidad del Jefe de la Unidad Técnica de Informática de la empresa, asegurar que todos los recursos de computación y Telecomunicaciones del Instituto, cuenten con planes de mantenimiento preventivo y/o correctivo debidamente contratados
- Queda terminantemente prohibido que los empleados y funcionarios 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.

CONCLUCION

Es un hecho que las políticas de seguridad son muy importantes implementarlas para que funcione una empresa u organización ya que son las que dan un orden, organización y obligaciones a los empleados. Es por ello que al crear una política de seguridad se debe tomar muchos factores y detalles importantes por muy mínimas que sean pueden afectar a la organización si se pasan desapercibidas.

BIBLIOGRAFIA

Libro: Políticas de Seguridad de Las Tecnologías de Información y Comunicaciones.pdf

https://www.ceupe.com/blog/ejemplo-politica-seguridad-informacion-y-sgsi.html