Política de Seguridad de la Información IMTCRD

Objetivo

Brindando importancia a la confidencialidad y seguridad de la información del IMTCRD, se considera implantar **tres mecanismos de seguridad (Prevención, Detección y Recuperación)**, con el objetivo de identificar amenazas y requerimientos tecnológicos para el buen manejo de la información.

Estos mecanismos proporcionaran un conjunto de reglas promulgadas para instituto las cuales garantizaran que todos los usuarios o redes de la estructura estén dentro del dominio y cumplan con las prescripciones relativas a la seguridad de los datos almacenados digitalmente.

Alcance

El alcance de este sistema debe ser aplicado por todos los empleados, contratistas, voluntarios y cualquier persona que tenga acceso permanente o temporal a los sistemas de hardware y software de la institución.

Se espera que los ejecutivos corporativos se interesen cada vez más directamente en la prevención de desastres de hardware y software, mejorando la credibilidad y reputación de la institución aumentando la confianza de la gestión administrativa.

Antes de implantar los mecanismos de seguridad para la institución, es necesario identificar y evaluar los siguientes elementos:

Identificación de Activos

- ✓ **Hardware:** Estaciones de trabajo, unidades de disco, equipos personales, routers, impresoras, líneas de comunicación, redes, servidores.
- ✓ **Software:** Sistemas operativos, programas fuente, antivirus, procesadores de texto y ofimática, software de comunicación, intranet.
- ✓ **Datos:** Durante la ejecución, almacenados en línea, backups, bases de datos, archivos de uso diario.
- ✓ **Documentación:** Sobre software, hardware, procedimientos administrativos locales.

ELABORÓ/PROYECTÓ: YISETH DIAZ
REVISÓ/APOTOBÓ: PATRICIA IREGUI

Identificación de Amenazas

- ✓ **Amenazas externas:** Se originan fuera de la institución como los virus, troyanos, gusanos y retaliaciones de ex-empleados o espionaje institucional.
- ✓ **Amenazas internas:** Son las amenazas que provienen del interior de la institución y que pueden ser muy costosas por que el infractor tiene mayor acceso y perspicacia para saber dónde reside la información sensible e importante. Las amenazas internas también incluyen el uso indebido del internet por parte de los empleados, también el uso de dispositivos electrónicos externos como memorias USB, teléfonos y tables personales.

Mecanismos de Seguridad y Privacidad

Una vez ya se hallan identificado los activos y amenazas, el siguiente paso es incorporar los mecanismos de seguridad, los cuales se dividen en tres grupos:

1. **Prevención:** Evitan desviaciones respecto a la política de seguridad.
2. **Detección:** Detectar las desviaciones si se producen, violaciones o intentos de violación de la seguridad del sistema.
3. **Recuperación:** Se aplican cuando se ha detectado una violación de la seguridad del sistema para recuperar su normal funcionamiento.

Dentro del grupo de mecanismos de prevención tenemos:

- **Control de acceso:** Los sistemas deben estar protegidos mediante mecanismos de control de acceso que establecen los tipos de acceso a la información para cualquier usuario o dependencia, para lo cual se debe implementar un servidor (archivos, aplicaciones) para controlar el acceso a la información para cada tipo de usuario o dependencia.

- **Seguridad en las comunicaciones:** La protección de la información (integridad y privacidad) cuando viaja por la red es especialmente importante y más aún con redes inalámbricas, por tanto, se debe implementar un Router o Firewall para filtrar y controlar las opciones de navegación (filtrado Ip, filtrado MAC, tags, etc…) y las credenciales de seguridad, las cuales deben ser actualizadas cada 2 meses.

- **Transferencia de datos:** Sirven para transferir datos entre equipos de oficina de manera segura sin que esto exponga los equipos y las credenciales de los mismos, el cual se puede implementar fomentando el uso de correos electrónicos seguros (corporativo), almacenamiento en la nube compartida (Google Drive, OneDrive, Mega, etc…) o en un directorio general el cual se incluiría en el servidor (Incluye niveles de usuario).

- **Asistencia:** Los usuarios deberán solicitar apoyo al área de Tecnología ante cualquier duda en el manejo de los recursos de cómputo de la institución.

- **Correos:** El correo electrónico no se deberá usar para envío masivo, materiales de uso no institucional o innecesarios entiéndase por correo masivo tales como cadenas, publicidad y propaganda comercial, política, social, etcétera.

- **BackUp y Seguridad:** Corresponde a la capacitación del personal de la institución con el objetivo de que puedan realizar copias de seguridad y a su vez cuidar, respetar y hacer uso adecuado de los recursos tecnológicos de la institución, también es necesario realizar una copia seguridad mensual, la cual debe estar fuera del área geográfica de la institución, este procedimiento se deberá ejercer en trabajo conjunto "Usuario - Técnico", para garantizar la fiabilidad del proceso.

- **Antivirus:** Según la hoja de vida cada uno de los equipos de la institución, el 100% de ellos utiliza sistemas operativos (S.O.) de la línea Microsoft, por tanto, se debe contar con software antivirus certificado por Microsoft.

A continuación, se deja el enlace con la lista de antivirus certificados por Microsotf:
https://support.microsoft.com/es-co/help/18900/consumer-antivirus-software-providers-for-windows

Nota// Los sistemas operativos con Windows 10, Windows 8.1 o Windows 8, cuentan con su propio antivirus (Windows Defender), es cual también es recomendado por el fabricante.

Control: Se debe realizar un chequeo mensual a todos los equipos para verificar que los anteriores mecanismos se encuentren funcionando, el cual se realizara por parte de la asistencia técnica o el área de sistemas encargada.

- Dentro del grupo de mecanismos de detección tenemos:

Antivirus: Se debe verificar que el antivirus se encuentre activo y a su vez realizar un chequeo semanal de las carpetas del sistema, este procedimiento deberá ser realizado por parte del usuario encargado del equipo, el cual será supervisado por el área de sistemas con base a los reportes generados por el antivirus.
Estado de hardware: Si el equipo presenta bloqueos, pantalla azul, apagado súbito o bajo rendimiento, se realizará una revisión general de las principales piezas de hardware para determinar si hay fallas.
Control: Se debe realizar un chequeo mensual a todos los equipos para verificar que todos los mecanismos preventivos (Seguridad de red, Reportes Antivirus, BackUps) se encuentren funcionando, el cual se realizara por parte de la asistencia técnica o el área de sistemas encargada.

- Dentro del grupo de mecanismos de recuperación tenemos:

Muchas de las amenazas que actualmente se encuentran en la red, causan o se disfrazan como problemas del S.O. como por ejemplo: Problemas con archivos DLL, bloqueos (también puede estar ligado a fallas de hardware), actividad inusual en el disco duro (Intermitencia del led indicador, también puede estar ligado a fallas de hardware), apagado súbito(también puede estar ligado a fallas de hardware), pantallas o ventanas desconocidas emergentes, archivos o carpetas ocultos, bajo rendimiento del equipo (también puede estar ligado a fallas de hardware), etc…
Por lo anterior, se deben realizar los siguientes procedimientos:

Antivirus: Realizar chequeo del equipo afectado y evaluar si el antivirus funciona correctamente con base a los reportes generados, este procedimiento deberá llevarse por parte del área técnica o el área de sistemas encargada.
BackUp: Realizar una copia de seguridad inmediata del equipo que se encuentre en riesgo, este procedimiento deberá llevarse por parte del área técnica o el área de sistemas encargada.

Revisión General: Si un equipo de la institución se ve infectado con un virus, se restringirá su acceso a la red durante el chequeo, luego se realizará una

revisión general de los demás equipos que se encuentran dentro de la misma red local, para poder determinar si también se encuentran en riesgo.

Estado de hardware: Si el equipo presenta bloqueos, pantalla azul, apagado súbito o bajo rendimiento, se realizará una revisión general de las principales piezas de hardware para determinar si hay fallas.
Para la implantación del mecanismo preventivo, deberá fijarse un cronograma que se ajuste al tiempo estipulado para la elaboración de cada una de las tareas por parte del área de sistemas, también se debe realizar una capacitación para el personal sobre la implementación de lo an