1 OBJETO

Proporcionar a los empleados, usuarios y partes interesadas una guía clara y concisa sobre cómo proteger adecuadamente la información y los datos críticos.

2 INTRODUCCIÓN

La seguridad de la información es fundamental para proteger los activos digitales de nuestra organización y garantizar la confidencialidad, integridad y disponibilidad de los datos. Este instructivo tiene como objetivo proporcionar pautas y mejores prácticas para mantener la seguridad de la información en nuestra organización

3 DEFINICIÓN

La seguridad de la información se refiere a la práctica de proteger la confidencialidad, integridad y disponibilidad de los datos y la información en una organización o sistema. Se trata de un conjunto de medidas y controles diseñados para salvaguardar los activos de información.

3.1 Confidencialidad:

La confidencialidad se refiere a la protección de la información para evitar que caiga en manos no autorizadas. Garantiza que solo las personas o entidades con los permisos adecuados tengan acceso a la información confidencial.

3.2 Integridad:

La integridad implica mantener la precisión y la consistencia de la información. Asegura que los datos no sean modificados o alterados de manera no autorizada o accidental, y que la información sea precisa y fiable.

3.3 Disponibilidad:

La disponibilidad se refiere a la accesibilidad de la información cuando se necesita. Esto implica garantizar que los sistemas y datos estén disponibles y funcionando correctamente, evitando interrupciones no planificadas.

4 RESPONSABILIDAD

4.1 Responsabilidad del personal de TI

Su responsabilidad es garantizar que los sistemas de tecnología de la información estén configurados, gestionados y protegidos de manera adecuada para salvaguardar la confidencialidad, integridad y disponibilidad de los datos y activos digitales. Algunas de las responsabilidades clave del personal de TI:

4.1.1 Gestión de Acceso y Autenticación:

- Administrar el acceso a sistemas y aplicaciones, asegurándose de que solo los usuarios autorizados tengan acceso.
- Implementar y mantener sistemas de autenticación seguros, como contraseñas fuertes, autenticación multifactor (MFA) y sistemas de gestión de identidad.

4.1.2 Protección contra Malware y Virus:

- Implementar soluciones de seguridad para detectar y prevenir malware, virus y otras amenazas cibernéticas.
- Mantener actualizado el software antivirus y realizar análisis regulares de seguridad.

4.1.3 Gestión de Vulnerabilidades y Parches:

- Identificar y gestionar vulnerabilidades en sistemas y aplicaciones.
- Aplicar parches de seguridad y actualizaciones de software de manera oportuna para proteger contra exploits conocidos.

4.1.4 Seguridad de la Red:

- Configurar y administrar firewalls, sistemas de detección de intrusiones y sistemas de prevención de intrusiones para proteger la red.
- Supervisar el tráfico de red en busca de actividades sospechosas.

4.1.5 Formación y concientización

- Programar capacitación en seguridad de la información en el plan anual
- Publicar tips para sensibilizar en temas de la seguridad de la información.

4.2 Responsabilidad del Personal

La seguridad de la información es responsabilidad de todos los empleados en la empresa, ya que todos tienen acceso a datos y sistemas que pueden ser vulnerables a amenazas cibernéticas y riesgos de seguridad. Cada miembro del personal desempeña un papel importante en la protección de la información de la empresa. Aquí se detallan algunas de las responsabilidades.

4.2.1 Gestión de Contraseñas:

- Crear y utilizar contraseñas fuertes y únicas para acceder a sistemas y cuentas.
- Cambiar las contraseñas periódicamente y no compartirlas con otras personas.

4.2.2 Seguridad de Dispositivos:

- Proteger sus dispositivos (computadoras, teléfonos móviles) con contraseñas o PIN.
- No dejar dispositivos desatendidos y asegurarse de que estén bloqueados cuando no se utilicen.

4.2.3 Correo Electrónico y Comunicaciones:

- Tener cuidado con los correos electrónicos de remitentes desconocidos y no abrir archivos adjuntos o hacer clic en enlaces sospechosos.
- No enviar información confidencial a través de correos electrónicos que no sea del correo corporativo de IST.

4.2.4 Uso de Redes y Internet:

- Conectarse solo a redes seguras y autorizadas.
- No visitar sitios web o descargar contenido de fuentes no confiables.

4.2.5 Protección de Documentos e Información:

- Almacenar documentos y archivos sensibles en ubicaciones seguras y protegidas (Servidores o discos duros de IST).
- No imprimir ni dejar documentos confidenciales en áreas accesibles.

4.2.6 Gestión de Dispositivos USB y Externos:

- No conectar dispositivos USB o unidades externas desconocidos en computadoras de trabajo sin autorización.
- Escanear dispositivos externos en busca de malware antes de usarlos en sistemas de la empresa.

4.2.7 Cumplimiento de Políticas y Procedimientos:

- Conocer y seguir las políticas y procedimientos de seguridad de la información de la empresa.
- Reportar cualquier incidente o actividad sospechosa de inmediato al departamento de TI o al responsable de seguridad.

4.2.8 Formación y Sensibilización:

- Participar en programas de formación en seguridad de la información.
- Mantenerse al tanto de las últimas amenazas y mejores prácticas en seguridad.

4.2.9 Colaboración:

- Colaborar con el equipo de TI y otras áreas o procesos para mantener y mejorar la seguridad de la información.
- Comunicar de manera efectiva cualquier problema o riesgo de seguridad identificado.

4.2.10 Responsabilidad Individual:

- Comprender que cada empleado es responsable de la seguridad de la información y que sus acciones pueden afectar la seguridad de toda la organización.

4.2.11 Reporte de Incidentes:

- Reportar de inmediato cualquier incidente de seguridad, como pérdida de dispositivos, violaciones de datos o actividades sospechosas.

5 PROCEDIMIENTOS

5.1 Control de acceso

Se revisará y darán los permisos correspondientes a las carpetas que están en el servidor y dependiendo el cargo se habilitara permisos especiales para la visualización de la información tanto de lectura como de escritura para estas carpetas. En la **M-013 Matriz de roles y permisos** se encuentra especificado.

5.2 Copias de seguridad

Se realiza copias de seguridad según lo establecido **I-027 Copia de Seguridad**.

5.3 Protección con Malware y virus

Se utiliza software antivirus y antimalware ESET Endpoint Security actualizado para proteger el sistema y los datos contra amenazas cibernéticas

5.4 Monitoreo

Se establece un sistema de monitoreo desde el Firewall para detectar y responder a actividades sospechosas o no autorizadas relacionadas con los accesos entrantes y salientes desde la red de internet hacia la intranet de IST y viceversa, este monitoreo consiste en visualizar la navegación que tiene cada uno de los equipos que se encuentran dentro de la oficina de IST.

5.5 Políticas de contraseña

Se establecerán políticas de contraseñas sólidas que requieran contraseñas únicas y complejas, y promueve la rotación periódica de contraseñas.

5.6 Autenticación multifactor (MFA)

Se implementa la autenticación multifactor siempre que sea posible para aumentar la seguridad de las cuentas de correo electrónico.

5.7 Protección física

Asegura que los servidores y dispositivos de almacenamiento físico estén protegidos contra el acceso no autorizado o el robo.

5.8 Actualizaciones y parches

Se mantendrán los sistemas operativos y software actualizados con los últimos parches de seguridad para evitar vulnerabilidades conocidas, según lo establecido en el instructivo **I-026 Mantenimiento Preventivo y Correctivo SW**

5.9 Aseguramiento de data personal retirado

El proceso IT se encarga de almacenar la información (Correos, OneDrive corporativo) retirado máximo por 30 días, el encargado de cada área del personal retirado debe informar si este tiempo debe ser modificado según sea el caso.

5.10 Aseguramiento de data proyectos

Cada coordinador de proyectos se encargará de guardar la información pertinente en el servidor, el proceso TI se responsabiliza de monitorear que el servidor tenga el espacio necesario para salvaguardar la información.

6 DOCUMENTOS RELACIONADOS

I-026 Mantenimiento Preventivo y Correctivo SW

I-027 Copia de Seguridad

M-013 Matriz de roles y permisos

CONTROL DE REVISIONES

REV. NO	FECHA	DESCRIPCIÓN	PREPARÓ	REVISÓ	APROBÓ
				QA/QC	GERENCIA
0	22-11-23	Nuevo instructivo	CACQ/VRC	DAPQ	CACT
1	25-04-24	Se relaciona la matriz de roles y permisos	VRC	DAPQ	CACT