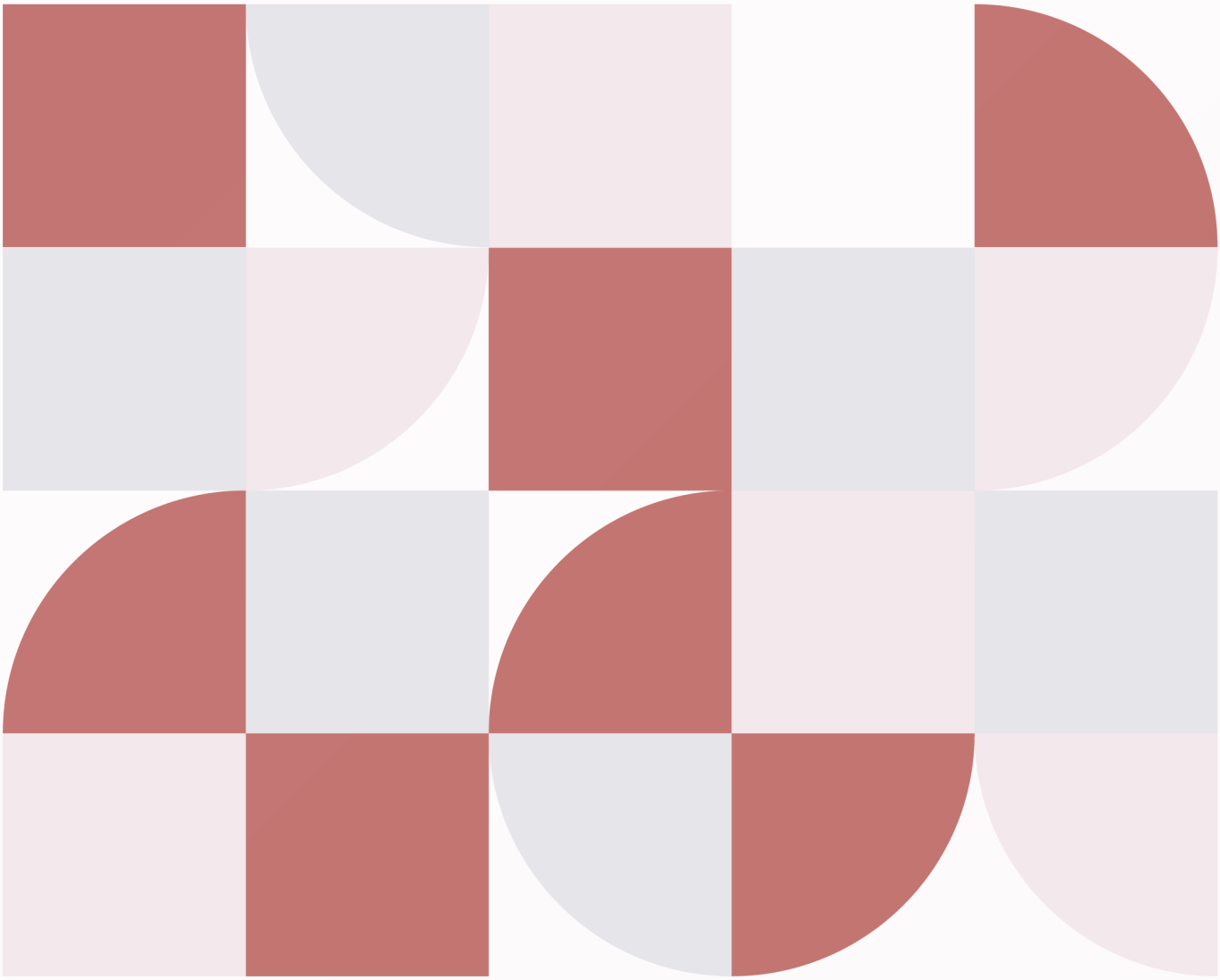
Ser Familia
Fundación

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Propiedad: Fundación Ser Familia Bolivia



BOLIVIA

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

1. Introducción

En el entorno actual, donde la digitalización de procesos desempeña un papel fundamental en todas las facetas de las operaciones, las políticas de seguridad informática se han convertido en un pilar para la protección de los activos digitales y salvaguardar la integridad de los datos sensibles.

En este contexto, las políticas de seguridad informática establecen un conjunto de normas y directrices que regulan la gestión de la seguridad de la información dentro de la empresa.

2. Objetivo

Las políticas de seguridad informática son un conjunto de reglas, directrices y procedimientos establecidos por una organización para proteger la información y los sistemas de tecnología de la información, contra amenazas y riesgos de seguridad.

Estas políticas definen las medidas de seguridad digital que se deben implementar, los roles y responsabilidades de los usuarios, los procedimientos para la gestión de incidentes y la respuesta a eventos de amenaza contra la seguridad.

Son esenciales para promover una cultura de seguridad organizacional y establecer un marco de trabajo que garantice la confiabilidad, integridad, disponibilidad y resguardo de la información.

3. Puntos que abarca

Dentro de los alcances se encuentran:

- Políticas de seguridad de contraseña.
- Políticas de Correo Electrónico.
- Política de respaldo de datos.
- Política de seguridad de la red.
- Política de educación y concientización.
- Políticas de actualización de software.
- Políticas de Mantenimiento de software y hardware

4. Desarrollo

POLÍTICAS DE SEGURIDAD DE CONTRASEÑA

Las políticas de contraseñas en seguridad informática son un conjunto de reglas y directrices que se crean con el objetivo de proteger el acceso a los sistemas, redes, aplicaciones y datos de la institución. Cuando el usuario obtiene una contraseña de acceso, esta cumplirá con una serie de requisitos para hacer más difícil que sea descifrada.

Las contraseñas deben ser creadas por el encargado de sistemas de Ser Familia la misma debe ser sólida y que dificulte a los ciberdelincuentes el proceso de descifrarlas, aplicando las siguientes directrices:

- Se creará contraseñas con un mínimo de 8 caracteres.
- Se alternará mayúsculas con minúsculas.
- Incluirá números y símbolos.
- No se utilizará fechas que recuerde el personal o que se le sean familiar.

Ejemplos: Card1na1/ - Cort4-p1k0

Las contraseñas deberán tener un periodo de caducidad y ser renovadas con una nueva en un tiempo determinado de 6 meses, cumpliendo todos los parámetros para su creación.

El resguardo de las contraseñas y la gestión deberá estar a cargo del encargado de sistemas con una copia de la lista de usuarios a Gerencia.

POLÍTICAS DE CORREO ELECTRÓNICO

Dentro del manejo de la información por correo electrónico debemos considerar que la administración de los mismos está a cargo del encargado de sistemas, incluyendo los siguientes puntos:

- Creación de correo bajo una dirección aceptable, por ejemplo: (xxxx@serfamiliabolivia.org)
- La contraseña será asignada por el encargado de sistemas.
- La configuración del mismo será por el encargado de sistemas.

Las directrices y el uso correcto del correo electrónico serán de conocimiento del usuario final, donde implica:

- El usuario no deberá enviar correos electrónicos con archivos adjuntos mayores a 10 mb.
- El usuario no podrá enviar correos electrónicos masivos o mayores a más de 4 destinatarios.
- El usuario contara con una firma digital estándar donde se encontrarán los datos de contacto.
- El usuario deberá consultar al encargado de sistemas en caso de tener dudas con el envío y recepción de correos en especial si se considera correo masivo.

POLÍTICA DE RESPALDO DE DATOS

Dentro de las políticas de backup, se definirá un lugar en el disco duro en una carpeta especifica que contenga la información de respaldo de cada usuario a nivel local. La misma debe ser copiada y almacenada en un dispositivo externo (disco duro externo) en periodos de cada 3 meses.

En caso de contar con almacenamiento en la nube se deberá verificar que cada equipo este sincronizado tanto en local como en la nube para resguardar la información generada en la Fundación Ser Familia.

POLÍTICA DE USO DE DISPOSITIVO EXTRAIBLE (Flash USB)

1. Propósito

Establecer directrices para el uso seguro de las memorias USB con el fin de proteger la información sensible y los recursos tecnológicos de la empresa.

2. Alcance

Esta política aplica a todos los empleados, contratistas y cualquier persona que utilice memorias USB en dispositivos propiedad de la empresa o conectados a la red corporativa.

3. Directrices Generales

- Uso Autorizado: Solo se permite el uso de memorias USB proporcionadas por la empresa. Las memorias USB personales están prohibidas.

- Escaneo de Virus: Todas las memorias USB deben ser escaneadas con el software antivirus de la empresa antes de usarse.

- Respaldo de Información: Los datos críticos no deben depender únicamente de una memoria USB; deben tener copias de seguridad adecuadas en servidores o sistemas de almacenamiento aprobados.

4. Acceso y Uso

- Restricciones de Acceso: Solo empleados autorizados pueden transferir datos a o desde memorias USB.

- Seguimiento y Monitoreo: La empresa puede monitorear el uso de memorias USB para asegurar el cumplimiento de esta política.

Reportes de Incidentes: Cualquier incidente de pérdida o robo de una memoria USB debe ser reportado inmediatamente al departamento de TI. o encargado de sistemas.

5. Responsabilidades

Deben cumplir con esta política y reportar cualquier uso indebido de memorias USB.

Las unidades de almacenamiento extraíble USB no deben ser insertadas en equipos externos a la institución, en caso que se requiera esta acción debe ser reportado al encargado de sistemas para ejecutar según procedimientos el uso dentro de la Fundación.

Todo usuario es responsable del uso y manejo de la información en estos dispositivos extraíbles.

6. Revisión y Actualización

Esta política será revisada y actualizada anualmente o según sea necesario para reflejar cambios en la tecnología y en las amenazas de seguridad.

POLÍTICA DE SEGURIDAD DE LA RED

Dentro de las políticas de seguridad de red, se deberá tener factores de protección como firewalls, antivirus y permisos definidos para optimizar la seguridad de la red, esto conlleva a definir si se compartirán carpetas o archivos en la red y quienes tendrán los accesos.

En caso de no tener archivos compartidos en red, el encargado de sistemas deberá verificar que los equipos estén debidamente configurados y con los firewalls de Windows activos y los parches y actualizaciones sean aplicados.

POLÍTICA DE EDUCACIÓN Y CONCIENTIZACIÓN

Es importante como en todo proceso que los usuarios finales estén enterados y conozcan de las diferentes políticas del uso de los recursos informáticos, para que de esta manera todos hagamos una red más segura y estable.

Es de suma importancia que los usuarios tomen conciencia del uso y no así del abuso del consumo de ancho de banda y que la navegación se limite a páginas que si necesita para el desarrollo de las actividades.

Es importante concientizar de los posibles ataques y vulnerabilidades que se tiene cuando nos exponemos a la navegación por internet, hacer conocer de las buenas prácticas y uso de los recursos, que hacer o cómo actuar ante posibles sospechas o incidencias.

Los usuarios no deberían utilizar flash memory ajeno a la institución, ya que este es el principal medio por el cual los equipos podrían quedar infectados o sufrir aluna vulnerabilidad.

POLÍTICAS DE ACTUALIZACIÓN DE SOFTWARE

Los sistemas operativos hoy en día tienen la bondad de recibir actualizaciones por internet, es importante tener un equipo y el sistema operativo siempre actualizado y con los constantes parches de seguridad que el mismo brinda

Por otro lado, el usuario debe estar consciente y capacitado que al existir actualizaciones en el sistema operativo estas deben ser aplicadas a la brevedad posible.

Todos los usuarios tendrán software en una versión estable y compatible con todos, se estandarizará las versiones y programas que se requieran para el desarrollo de sus actividades diarias. (Office misma versión)

POLÍTICAS DE MANTENIMIENTO DE SOFTWARE Y HARDWARE

Es importante realizar un plan de manteamiento de software y hardware para preservar de manera correcta los dispositivos de hardware y diversos periféricos con los que cuente el usuario. A su vez se realizará un mantenimiento a nivel software del sistema operativo para eliminar archivos temporales, limpieza de cookies de navegación y cualquier archivo que se genere y derive en el consumo de memoria o de algún recurso de la PC

Se realizará un cronograma de mantenimiento de software y hardware con un periodo de 6 meses, o dos veces al año, este se dividirá por áreas o por encargado de equipo, el mismo estará a cargo del encargado de sistemas en coordinación con el usuario final.

CONCLUSIONES Y RECOMENDACIONES

Las políticas de seguridad se deben aplicar para todos, y en todos los niveles, definiendo los permisos y privilegios ya sean por perfiles de usuarios, personas o cargos. Para preservar la integridad y protección de los datos se recomienda adquirir antivirus con licencia.

Para asegurar el buen funcionamiento de los equipos y el ordenado de datos se recomienda el formateo y la reinstalación de todos los equipos, de esta manera uniformizar los programas instalados y que todos cuenten con las mismas versiones de office y otras herramientas, un sistema operativo limpio y libre de parches no propios del Windows garantiza el buen desempeño y funcionamiento.

Se evidencio que los usuarios no cuentan con restricciones de navegación y consumo del ancho de banda, se recomienda que se haga énfasis en los usuarios que no deben ingresar a paginas como YouTube, videos en línea, radio en línea o sus derivados ya que esto hace que se eleve el tráfico en el consumo del ancho de banda haciendo que otros usuarios tengan más retraso en tiempos de respuesta en su navegación por internet.

En caso que el usuario utilice su computadora personal ajena a la institución, se recomienda que el mismo realice copias de la información generada una vez a la semana, ya que, al usar un equipo personal, este debe tener otro tratamiento, donde no se puede contar con una contraseña para acceso libre en cualquier instante y mucho menos acceder a la información el momento que se requiera, son limitantes que podrían ocasionar la posible pérdida de información.

Se recomienda elaborar un contrato de confidencialidad de la información, donde se estipule el manejo y cuidado de la misma, la autoría y propiedad que son cedidos para la institución, el buen uso de los recursos informáticos y cada usuario de su visto bueno y firma como parte de su contrato laboral.

Todos los usuarios son responsables del manejo de la información, cualquier incidente o perdida de información se procederá a la evaluación del incidente para determinar el grado de responsabilidad del usuario y de esta manera aplicar las sanciones correspondientes.

Se recomienda mejorar la seguridad de las cámaras, instalando y ampliando la vigilancia en los puntos más relevantes para tener una mejor cobertura.