CIBERSEGURIDAD

ECOVA 2024

¿Por qué nos importa la ciberseguridad?

PORQUE VALORAMOS NUESTROS DATOS

Principios de seguridad de la información

Confidencialidad

La confidencialidad es un principio de seguridad de la información que se refiere a la protección de la información sensible y privada contra accesos no autorizados. Esto se logra a través de técnicas de autenticación y autorización, como contraseñas y control de acceso.

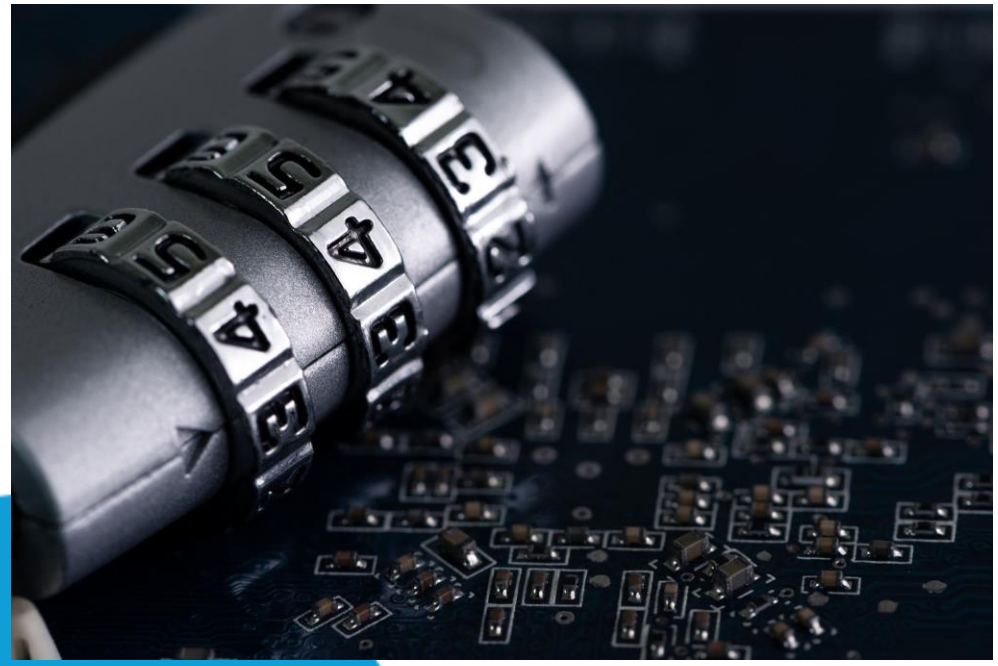
Integridad

La integridad es un principio de seguridad de la información que se refiere a la precisión y consistencia de los datos. Se protege la integridad de la información mediante la detección y prevención de la modificación no autorizada de los datos.

Disponibilidad

La disponibilidad es un principio de seguridad de la información que se refiere a la capacidad de acceder y utilizar la información cuando sea necesario. La disponibilidad se protege a través de la planificación de la continuidad del negocio y la implementación de medidas de recuperación ante desastres.

Normas básicas para proteger tu empresa



Actualiza regularmente tu software

Mantener actualizado el software de la empresa es importante para protegerla de vulnerabilidades. Actualiza regularmente el software y los sistemas operativos para asegurarte de que la empresa esté lo más protegida posible.

Usa contraseñas seguras

Las contraseñas seguras son un aspecto importante de la ciberseguridad. Utiliza contraseñas complejas, cambia las contraseñas periódicamente y no compartas tus contraseñas con nadie.

Limita el Acceso de los Usuarios a los Datos

Limitar el acceso de los usuarios a los datos es una medida importante de seguridad. Solo otorga acceso a los datos y sistemas que cada usuario necesita para realizar su trabajo y asegúrate de que los empleados tengan la seguridad adecuada para acceder a ellos.

Formación en ciberseguridad

La formación en ciberseguridad puede ayudar a los empleados a comprender las amenazas y a tomar medidas preventivas. Realiza capacitaciones y talleres de forma periódica para garantizar que todos los empleados estén actualizados sobre las últimas tendencias y amenazas en ciberseguridad.

ACTUALIZA EL SOFTWARE

USA CONTRASEÑAS SEGURAS

- No uses la misma para todo, aunque sea bueniiiisima. Have i pawned.
- No la compartas con absolutamente nadie.
- Activa 2mfa.
- Usa un gestor de contraseñas. NOOO, excel es para otra cosa!!!!
- Los post-it no se inventaron para apuntar contraseñas.
- Cambia las contraseñas de vez en cuando. (no cada 5 años).

Demo excel contraseñas

- Comprobar contraseñas más usadas en el mundo.
- Have i pawned.
- Demo excel contraseñas.

Se preventivo con la ciberseguridad.

- **Usa endpoints**.Nooo, un antivirus ya no vale.
- Si es gratis no vale!.
- **Usa firewalls** pero que esten bien configurados.
- **Monitoriza...** (toma decisiones con datos).
- **Auditate**.

Firewall

- Un firewall es una barrera de seguridad que puede proteger su red y sus dispositivos de acceso no autorizado.
- Demo firewall en tiempo real.
- Demo shodan. server: Sunny WebBox
- **port:445 country:es authenticati on: disabled**

Protege tu puesto de trabajo.

- Software pirata = red botnet.
- Sin permisos de administrador.
- No recordar la contraseña en navegadores.
- No uses la wifi de nadie y menos para ver la cuenta del banco.
- Cifra datos sensibles.
- Audita accesos según rol o usuario. ¿Todo el mundo debe ver todo?.
- Huye de hosting lowcost.
- Usa virus total como segunda opinion.

Copias de seguridad

Mi única solucion ante un desastre.

¿Por qué hacer copias de seguridad?

Protección de datos

Las copias de seguridad protegen los datos de una empresa de fallos del sistema, errores humanos, ataques de malware, desastres naturales y otras amenazas que puedan comprometer la integridad y disponibilidad de los datos.

Recuperación de datos

Las copias de seguridad permiten recuperar los datos perdidos en caso de fallo del sistema, ataques de malware o desastres naturales, lo que garantiza la continuidad del negocio y minimiza la interrupción operativa.

Identificar los datos críticos

Datos Financieros

Los datos financieros, como las transacciones bancarias y los registros contables, son críticos para la gestión y el éxito de cualquier empresa. Estos datos son especialmente importantes para las empresas que dependen de la facturación y el flujo de efectivo para su funcionamiento diario.

Información personal de los empleados

La información personal de los empleados, como los registros de nómina y los datos de contacto de emergencia, es esencial para el mantenimiento de un entorno laboral seguro y productivo. Además, la pérdida o el robo de esta información puede dar lugar a riesgos de seguridad para los empleados y la empresa en su conjunto.

Datos de clientes

Los datos de los clientes, como los registros de transacciones y la información de contacto, son críticos para la gestión de la relación con los clientes y para la generación de negocios en el futuro. Además, la pérdida o el robo de esta información puede dañar la reputación de la empresa y poner en riesgo la confianza del cliente.

Frecuencia de las copias de seguridad

La frecuencia de las copias de seguridad depende de la cantidad de cambios que se realicen en los datos. Para los datos críticos, es recomendable hacer copias de seguridad diarias o más frecuentes, mientras que para los datos menos críticos se puede hacer una copia semanal o mensual.

Métodos de almacenamiento

Discos duros externos

Los discos duros externos son una opción popular y económica para las copias de seguridad. Son portátiles, fáciles de usar y ofrecen una gran capacidad de almacenamiento pero no es la solucion profesional para una empresa.

Servidores en la nube

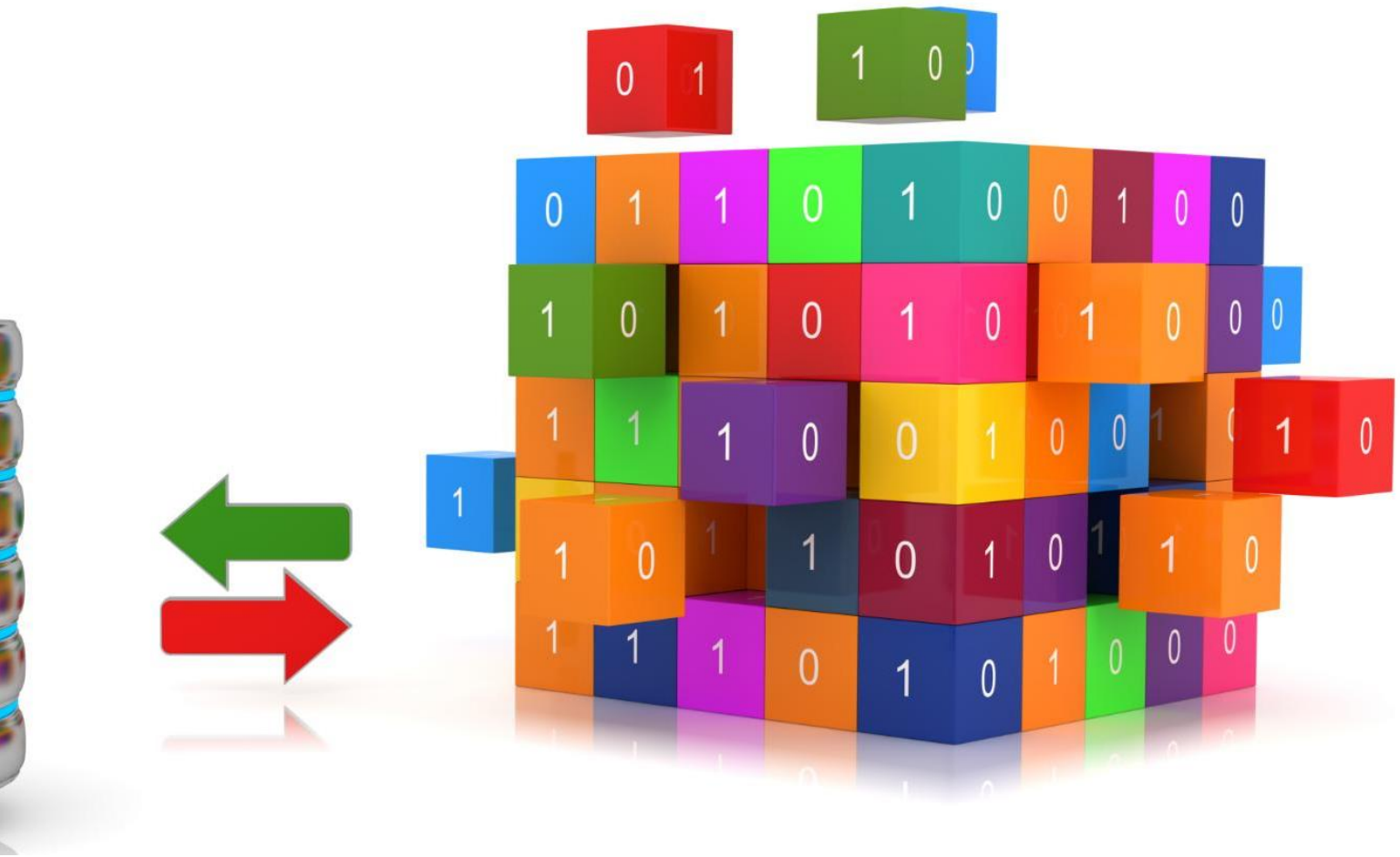
Los servidores en la nube son una opción conveniente y escalable para las copias de seguridad. Proporcionan acceso remoto y seguro a los datos desde cualquier lugar y en cualquier momento.

Nas

Los nas son cajas inteligentes con uno o varios discos dentro que me permiten gestionar las copias pero no tendrian sentido sin que haya una replica offsite.

Automatización de las copias de seguridad

La automatización de copias de seguridad permite ahorrar tiempo y reducir errores al programar copias automáticamente en el momento adecuado. Es importante elegir una herramienta de copias de seguridad que permita programar las copias automáticamente y enviar **notificaciones en caso de error.**



Pruebas de recuperación

Las pruebas regulares de recuperación de datos son esenciales para garantizar que las copias de seguridad estén funcionando correctamente y puedan recuperar los datos perdidos en caso de fallo del sistema. Estas pruebas deben ser documentadas adecuadamente para una rápida recuperación en caso de una interrupción del negocio.

Plan de contingencia

Paso a seguir en caso de fallo del sistema

Un plan de contingencia debe incluir los pasos a seguir en caso de fallo del sistema, identificando los riesgos y estableciendo procedimientos de emergencia para mitigarlos.

Recuperación de Datos

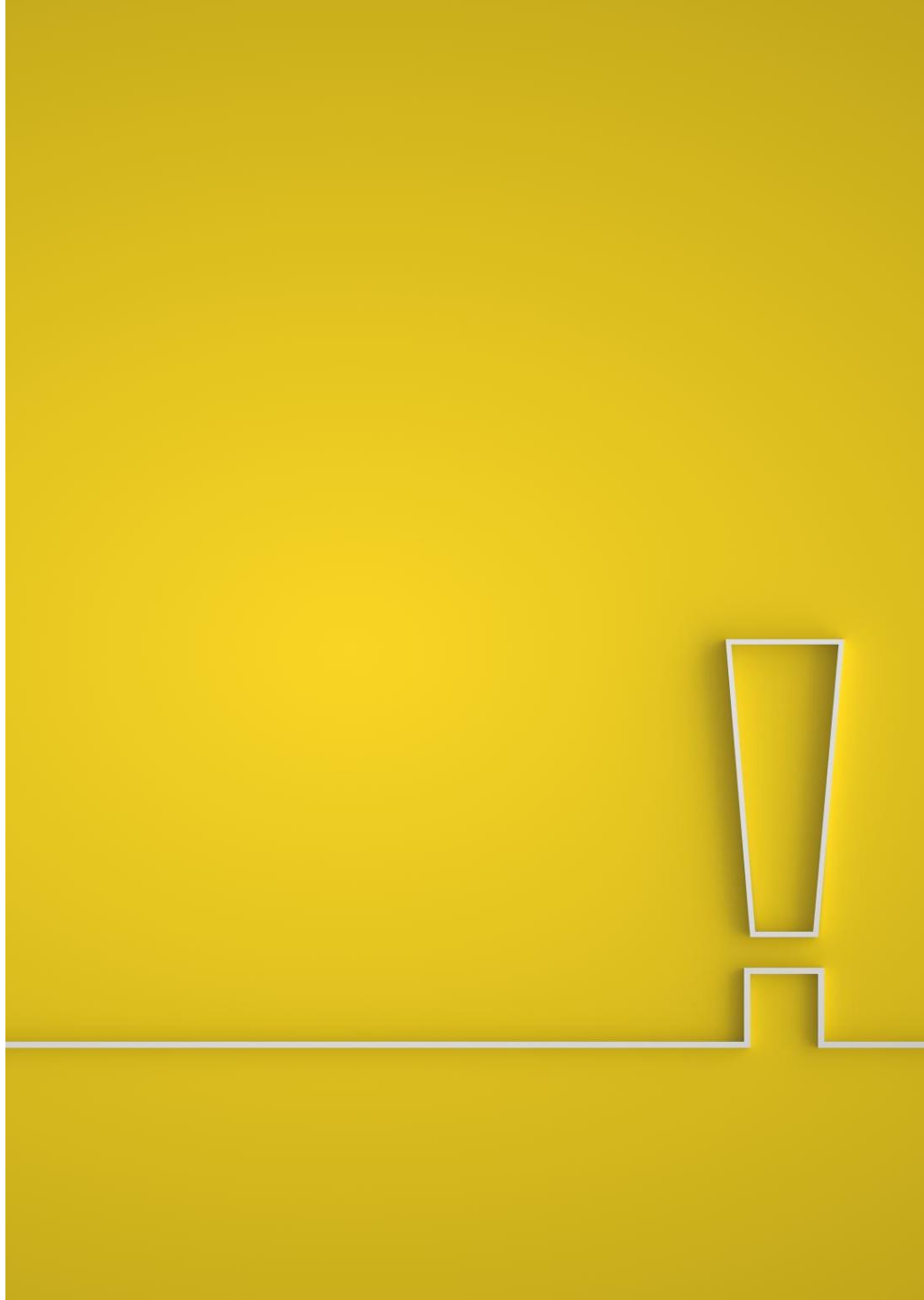
Un plan de contingencia debe incluir un plan de recuperación de datos para garantizar la continuidad del negocio en caso de pérdida de datos. Este plan debe incluir copias de seguridad y medidas de recuperación.

Comunicación con Empleados y Clientes

Un plan de contingencia debe incluir un plan de comunicación para garantizar que los empleados y clientes estén informados y actualizados en caso de un desastre.

Conclusiones

Las copias de seguridad son esenciales para proteger los datos y garantizar la continuidad del negocio. Es importante identificar los datos críticos, elegir el tipo de copia de seguridad adecuado, automatizar las copias y realizar pruebas de recuperación. Un plan de contingencia permitirá estar preparados en caso de desastre.



IMPORTANCIA DE LA CIBERSEGURIDAD EN LA PROTECCIÓN DE CORREO ELECTRÓNICO

on el correo electrónico.
an información
a sus clientes.

electrónico. Las
de malware, lo que

La suplantación de identidad es un riesgo común asociado con el correo electrónico. Los hackers pueden enviar mensajes que parecen provenir de una fuente confiable, lo que puede llevar a la revelación de información confidencial o a la descarga de malware.

Políticas de seguridad de correo electrónico

Encriptación de correos electrónicos

La encriptación de correos electrónicos es una política de seguridad vital para proteger la información confidencial en tránsito. Se utiliza para asegurar que solo el destinatario previsto pueda leer el contenido del correo electrónico.

Restricción de acceso a correos electrónicos

La restricción de acceso a ciertos correos electrónicos es una política de seguridad que asegura que solo las personas con permisos adecuados pueden acceder a la información confidencial contenida en los correos electrónicos.

Eliminación segura de correos electrónicos antiguos

La eliminación segura de correos electrónicos antiguos es una política de seguridad necesaria para proteger la información confidencial en reposo. Se asegura de que los correos electrónicos antiguos se eliminen de manera segura y permanente, evitando cualquier posible acceso no autorizado en el futuro.