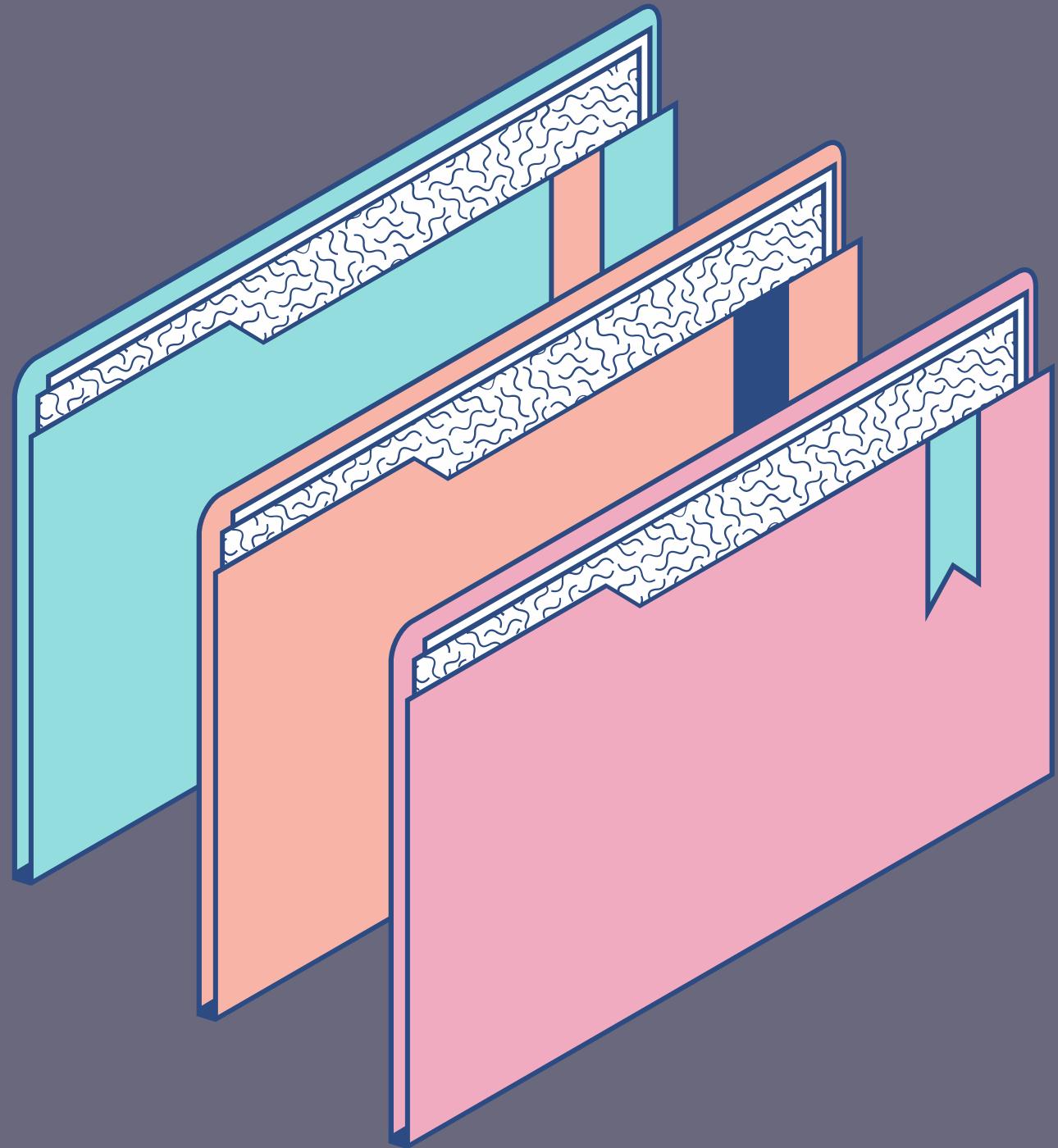


# Capacitación

## .CKS 2024



# Agenda



## TEMAS PRINCIPALES DE ESTA PRESENTACIÓN

- Introducción a la Seguridad de la Información
- Manejo de Contraseñas
- Acceso a la Red y Sistemas
- Seguridad Física y Protección de Dispositivos
- Reconocimiento y Respuesta a Amenazas
- Protección de Datos y Privacidad
- Uso Seguro de Internet y Correo Electrónico
- Simulaciones y Ejercicios Prácticos
- Recursos y Soporte

# Introducción a la Seguridad de la Información

La seguridad de la información es crucial para cualquier empresa en la era digital actual. Se refiere a proteger la información sensible y los sistemas que la manejan de accesos no autorizados, daños o cualquier otra amenaza que pueda comprometer su confidencialidad, integridad y disponibilidad.





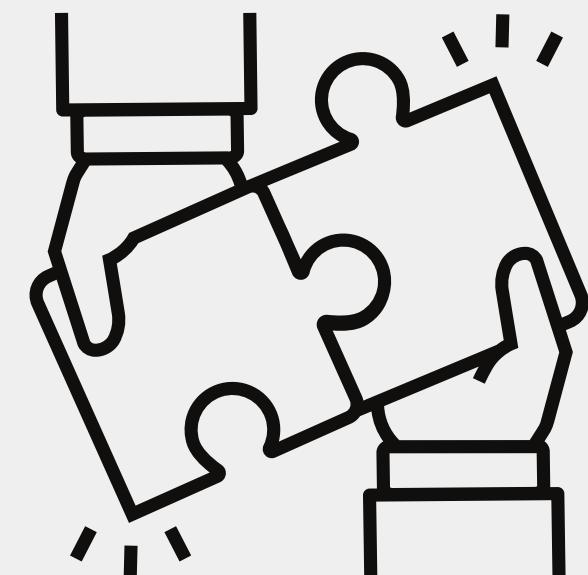
## Confidencialidad

- Garantiza que la información solo esté disponible para aquellos autorizados a acceder a ella.
- Se logra mediante la implementación de controles de acceso y cifrado para proteger los datos contra accesos no autorizados.



## Integridad

- Asegura que la información sea precisa, completa y no haya sido modificada de manera no autorizada
- Se logra mediante la implementación de controles para detectar y prevenir la alteración no autorizada de los datos.



## Disponibilidad

- Garantiza que la información esté disponible y accesible cuando sea necesario por aquellos que están autorizados a utilizarla.
- Se logra mediante la implementación de medidas para prevenir interrupciones del sistema.



# Manejo de Contraseñas

El manejo de contraseñas se refiere al conjunto de prácticas y procedimientos utilizados para crear, almacenar, proteger y gestionar contraseñas de manera segura.

El objetivo del manejo de contraseñas es proteger la información personal y asegurar la privacidad y seguridad de las cuentas en línea frente a posibles amenazas como el robo de identidad y el acceso no autorizado.





# Importancia de contraseñas fuertes y únicas

- Protegen cuentas y datos sensibles de accesos no autorizados.
- Deben ser largas, complejas y únicas para cada cuenta.

## Cómo crear y gestionar contraseñas seguras

- Usa frases memorables o cadenas aleatorias.
- Evita información personal y comparte contraseñas.
- Cambia contraseñas periódicamente y usa autenticación de dos factores (2FA).

## Uso de herramientas de gestión de contraseñas

- Almacenan y gestionan contraseñas de forma segura.
- Encriptan contraseñas y las protegen con una contraseña maestra.
- Facilitan la generación de contraseñas fuertes y el inicio de sesión seguro.
- Ejemplos: LastPass, Dashlane, 1Password, Bitwarden.



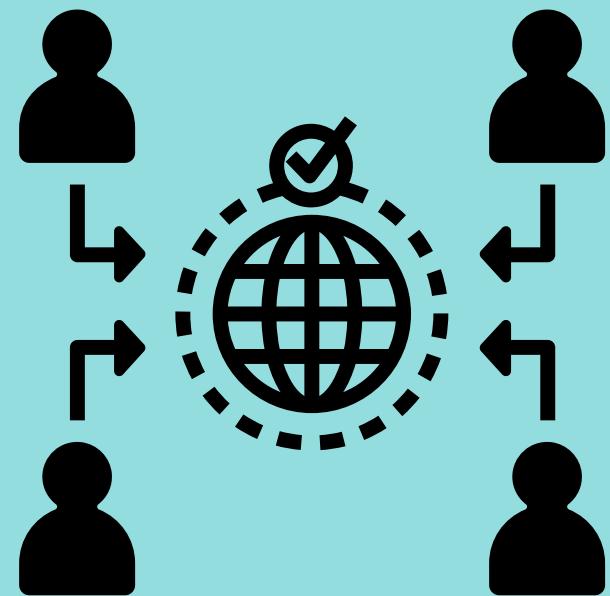
## Acceso a la Red y Sistemas

El "Acceso a la Red y Sistemas" se refiere a la capacidad de usuarios y dispositivos para conectarse y utilizar recursos en una red informática y sistemas relacionados, incluyendo Internet y redes locales.

La seguridad de este acceso es crucial y se logra mediante la autenticación, autorización y control de los recursos disponibles, utilizando medidas como firewalls y sistemas de autenticación.

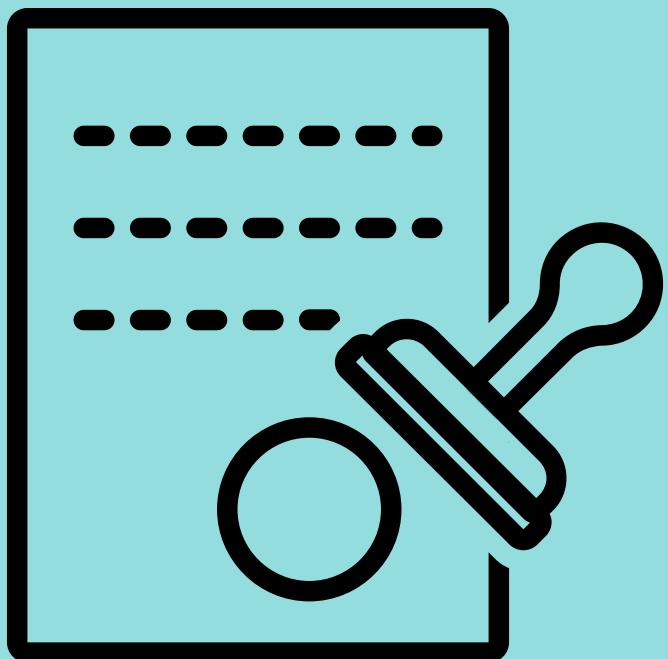
## Políticas de acceso a la red y sistemas de la empresa

- Definen quién tiene acceso a qué y qué acciones están permitidas.
- Comunicación clara y refuerzo a través de la formación.



## Procedimientos de solicitud y gestión de permisos

- Incluyen formularios de solicitud, aprobaciones y documentación.
- Garantizan transparencia y rendición de cuentas.



## Importancia de cerrar sesión y bloquear dispositivos

- Previene accesos no autorizados y protege la privacidad.
- Evita el acceso no deseado cuando los dispositivos están inactivos.



# Seguridad Física y Protección de Dispositivos

Se refiere a la protección de los recursos físicos y dispositivos tecnológicos de una organización contra robos, daños y acceso no autorizado.

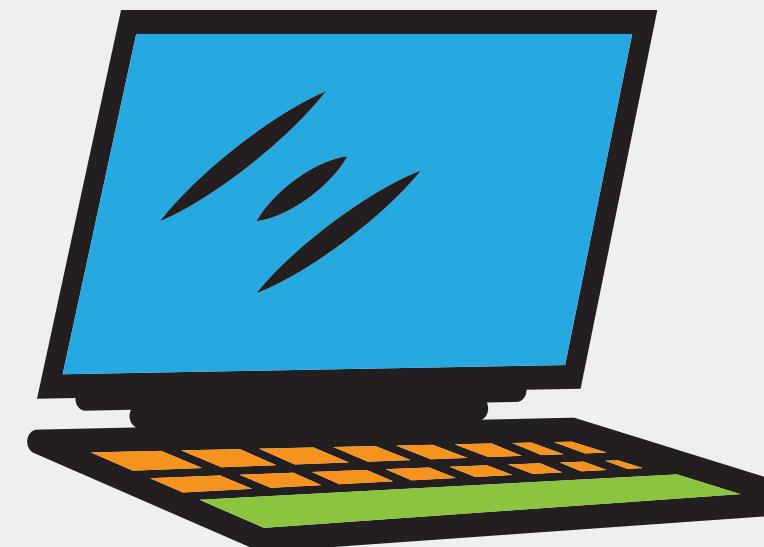
Esto incluye el aseguramiento de instalaciones físicas y la implementación de medidas de seguridad para proteger dispositivos como computadoras y servidores.





## Seguridad física de equipos de trabajo

- Mantenerlos en áreas seguras y protegidas.
- Evitar dejar dispositivos desatendidos en áreas públicas.



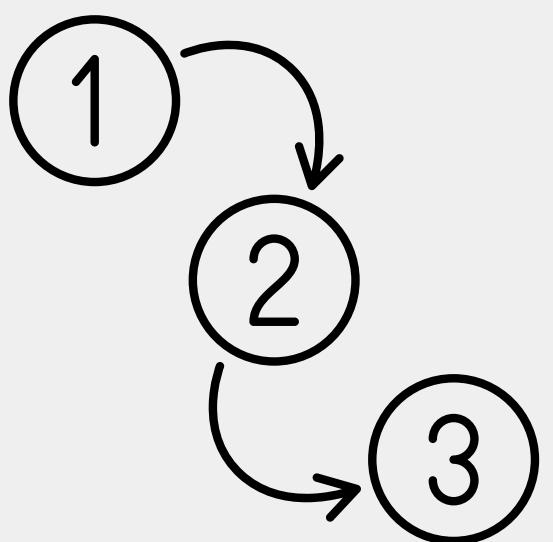
## Uso seguro de dispositivos móviles y laptops

- Establecer políticas de seguridad claras.
- Capacitar a los empleados en prácticas seguras.



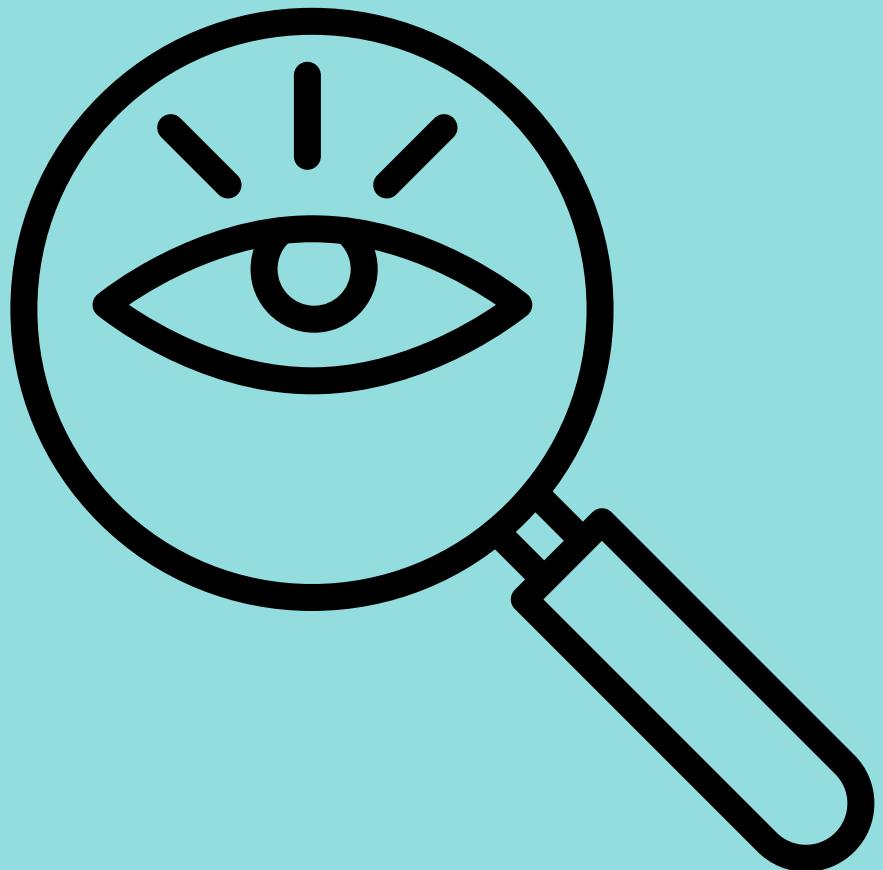
## Reporte de dispositivos perdidos o robados

- Establecer procedimientos claros y rápidos.
- Informar de inmediato la pérdida o robo para tomar medidas de protección.



# **Reconocimiento y Respuesta a Amenazas**

Se refiere a detectar y enfrentar posibles peligros para la seguridad de la información y los sistemas de una organización. Esto implica identificar actividades sospechosas y tomar medidas para mitigar el impacto de las amenazas, como bloquear el acceso no autorizado o eliminar malware.



# Tipos comunes de amenazas cibernéticas

- Phishing: Engaño para obtener información personal a través de correos o sitios web falsos.
- Malware: Software malicioso que daña o infecta sistemas.
- DDoS: Sobrecarga de tráfico para interrumpir sistemas o redes.
- Ingeniería social: Manipulación psicológica para obtener información confidencial o acciones específicas.



# Cómo reconocer correos electrónicos y mensajes sospechosos

- Revisa errores gramaticales
- Verifica remitentes
- Desconfía de enlaces o archivos adjuntos no solicitados.



# Procedimientos para reportar incidentes y amenazas

- Establece canales claros de comunicación.
- Capacita a los empleados para reportar incidentes.
- Implementa un proceso de respuesta a incidentes.



# Protección de Datos y Privacidad

Se refiere a detectar y enfrentar posibles peligros para la seguridad de la información y los sistemas de una organización. Esto implica identificar actividades sospechosas y tomar medidas para mitigar el impacto de las amenazas, como bloquear el acceso no autorizado o eliminar malware.



# Manejo seguro de datos personales y sensibles

- Almacenamiento, procesamiento y transmisión seguros.
- Medidas como el cifrado y el acceso restringido.



# Cumplimiento con leyes y regulaciones de protección de datos

- Respetar normativas como el GDPR o la Ley de Protección de Datos Personales.
- Evitar sanciones legales y proteger la reputación.



# Importancia de la privacidad de la información de clientes y empleados

- Construir y mantener la confianza.
- Evitar pérdida de clientes, daño a la reputación y sanciones legales.



# Uso Seguro de Internet y Correo Electrónico

Esto implica tomar medidas para protegerse en línea, como usar contraseñas seguras, verificar la autenticidad de los sitios web, y evitar abrir correos electrónicos o hacer clic en enlaces sospechosos.



# Navegación segura en internet

- Mantén programas y sistemas actualizados.
- Usa conexiones seguras y contraseñas fuertes.
- Evita hacer clic en enlaces o descargar archivos sospechosos.
- Sé cauteloso al compartir información personal en línea.



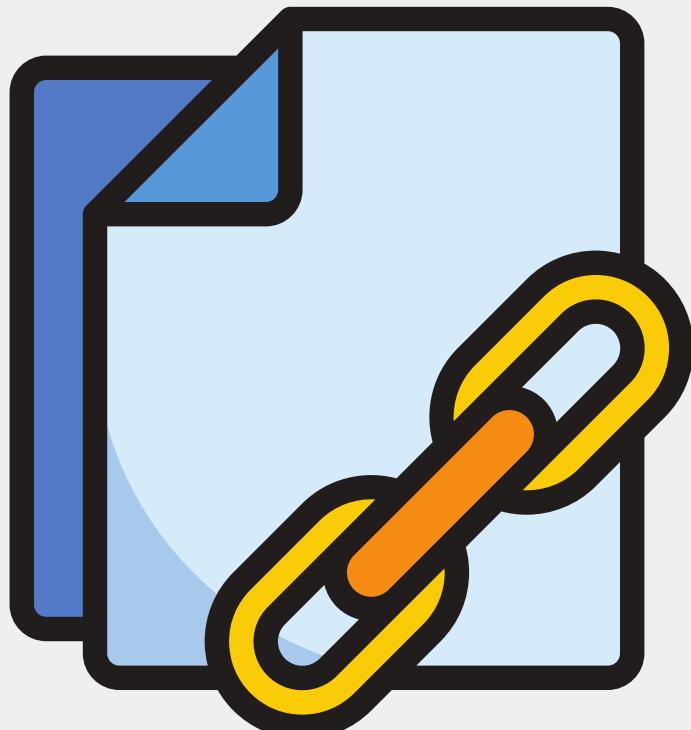
# Uso del correo electrónico corporativo

- No compartas información confidencial sin verificar la identidad del destinatario.
- Evita abrir correos de remitentes desconocidos y no solicitados.
- No descargues archivos ni hagas clic en enlaces sospechosos.



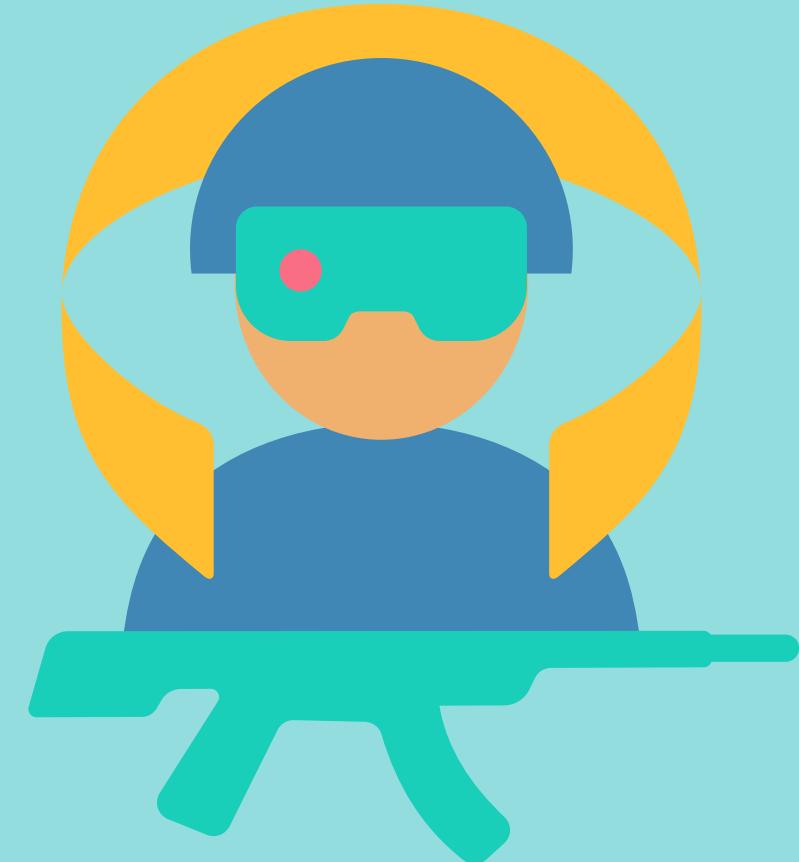
# Precauciones con archivos y enlaces:

- Verifica la autenticidad de las fuentes antes de descargar archivos o hacer clic en enlaces.
- Usa software antivirus actualizado.
- Evita enlaces acortados y previsualiza las URL completas cuando sea posible.



# **Simulaciones y Ejercicios Prácticos**

Son actividades de entrenamiento que ofrecen experiencia práctica en situaciones controladas, como ciberataques o emergencias, para mejorar la preparación y habilidades de respuesta de las personas.



# Simulaciones de amenazas

- Imitan ataques reales para evaluar la conciencia y preparación de los empleados.
- Evalúan la respuesta ante correos falsos que imitan ataques de phishing



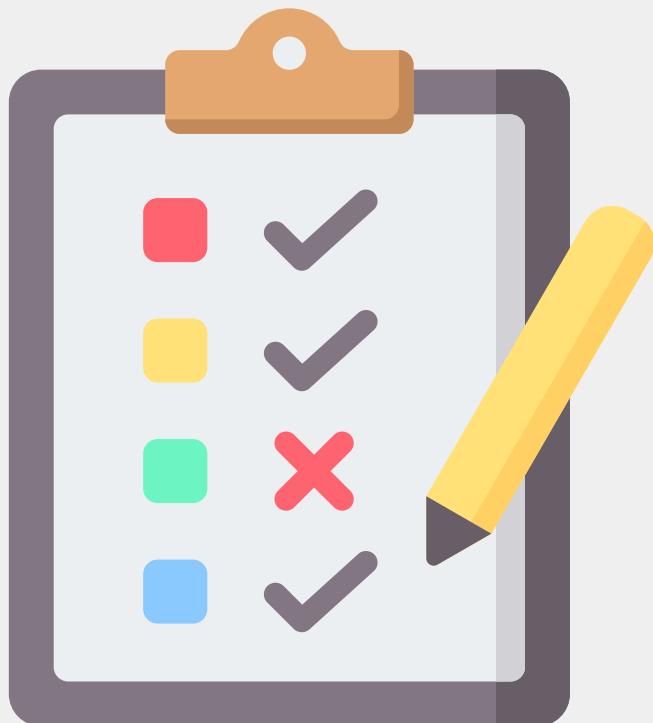
# Ejercicios de respuesta a incidentes

- Simulan incidentes de seguridad para evaluar la capacidad de respuesta.
- Pon a prueba la detección, contención y mitigación de amenazas.



# Evaluaciones de conocimientos adquiridos

- Miden la comprensión y aplicación de conocimientos de seguridad.
- Incluyen cuestionarios, exámenes prácticos o estudios de caso.



# Recursos y Soporte

Engloba una amplia gama de servicios y herramientas destinadas a facilitar diversas actividades y resolver problemas.

Estos recursos pueden abarcar desde el acceso a personal especializado, como expertos en tecnología o asesores legales, hasta la disponibilidad de herramientas y tecnologías específicas, como software o equipos.



# Información de contacto para soporte técnico y seguridad

- Proporciona un punto de contacto claro y accesible.
- Incluye correos electrónicos, números de teléfono u otras plataformas de gestión de incidencias.



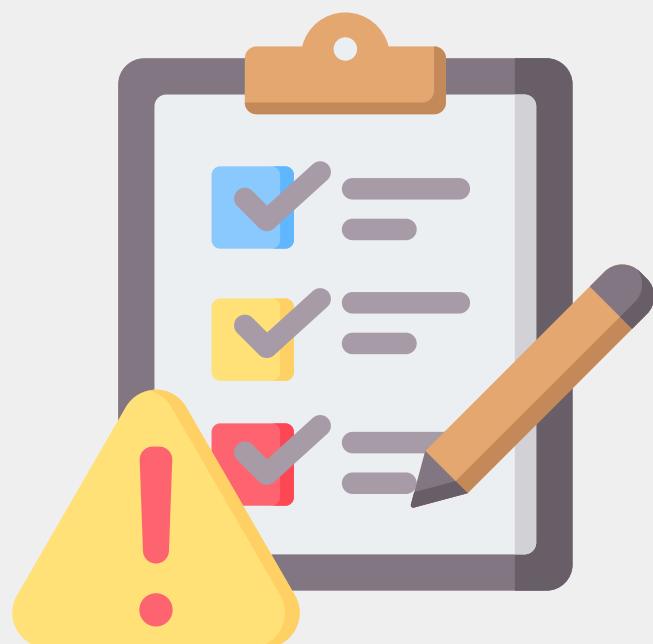
# Recursos adicionales para aprender sobre seguridad de la información

- Ofrece cursos en línea, materiales educativos, blogs y webinars.
- Fomenta la participación en grupos de discusión y comunidades en línea.



# Procedimientos para reportar problemas de seguridad

- Establece un proceso claro y sencillo para reportar problemas.
- Incluye instrucciones detalladas sobre qué información proporcionar y cómo se gestionarán los informes.



GRACIAS