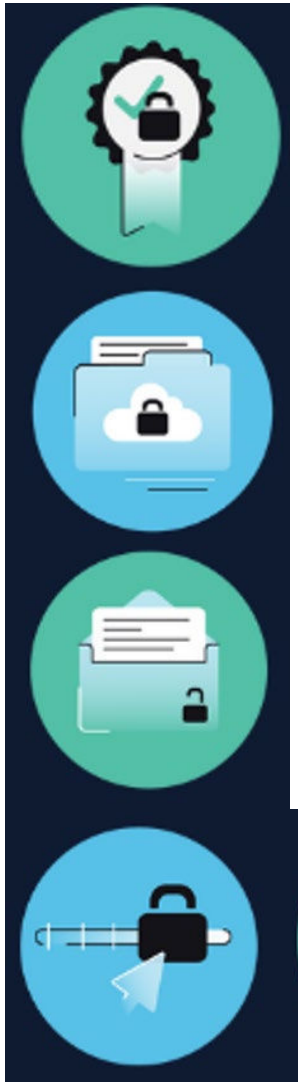
INTER

Concienciación sobre la Seguridad Cibernética

Septiembre 2026

Concienciación sobre la Seguridad Cibernética



Piensa antes de hacer clic

No caigas en estafas de phishing. Reconoce y denuncia los correos electrónicos sospechosos.

Usa contraseñas fuertes

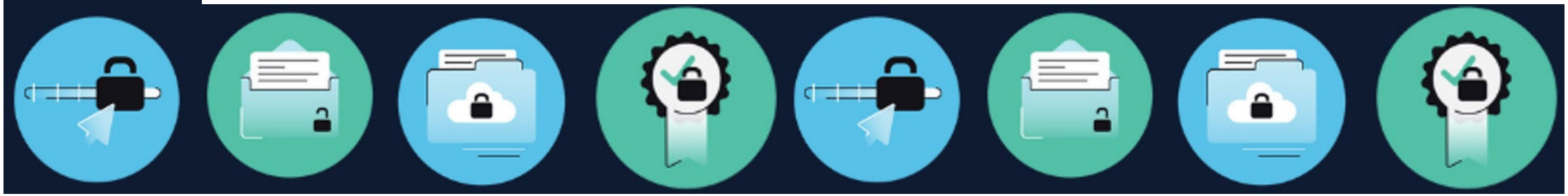
Utiliza contraseñas largas, únicas y generadas aleatoriamente. Utiliza administradores de contraseñas para almacenarlas.

Actualiza tu software

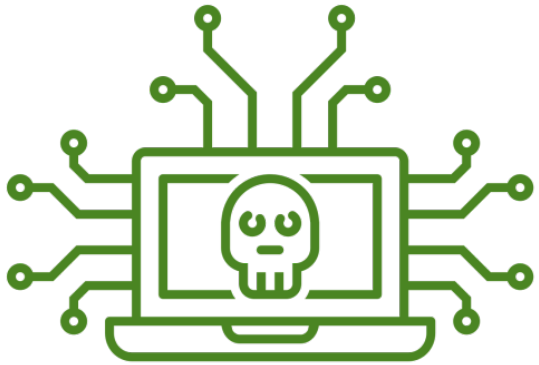
Actúe rápidamente para actualizar el software; mejor aún, activa las actualizaciones automáticas.

Habilita MFA

Exigir a los usuarios que habiliten MFA para iniciar sesión hace que sea mucho menos probable que sean hackeados.



Tipos de Ataque Cibernético

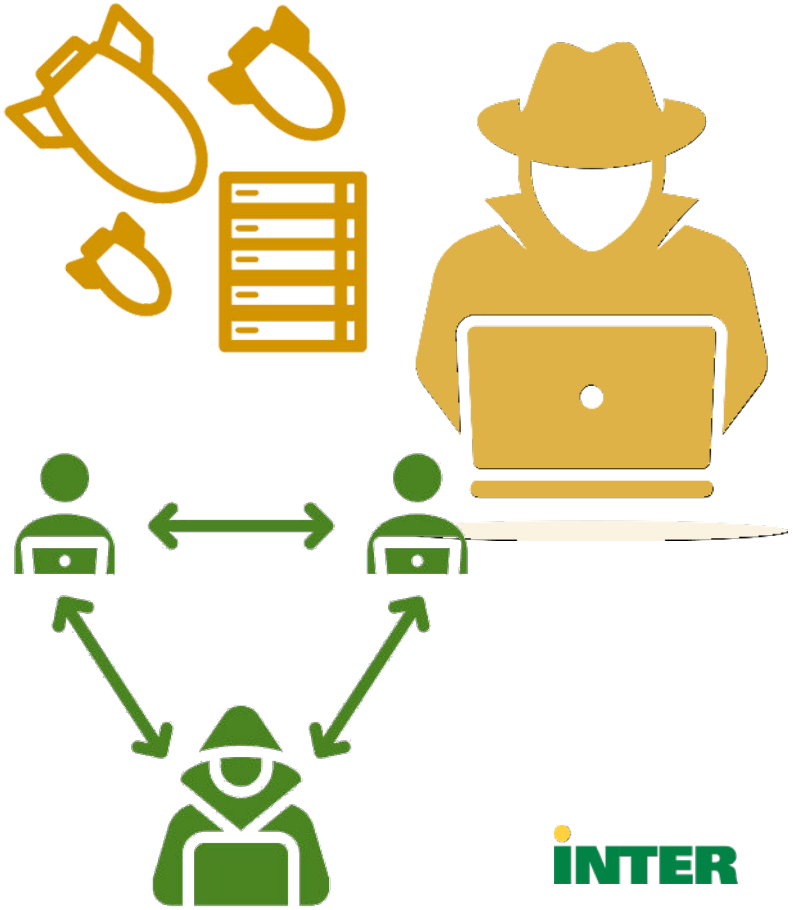


Malware

El 9% de los ataques cibernéticos que tuvieron lugar en los últimos 12 meses se debieron a infracciones de malware.

Denegación de servicios

El 8% se debió a ataques de denegación de servicio (DOS).



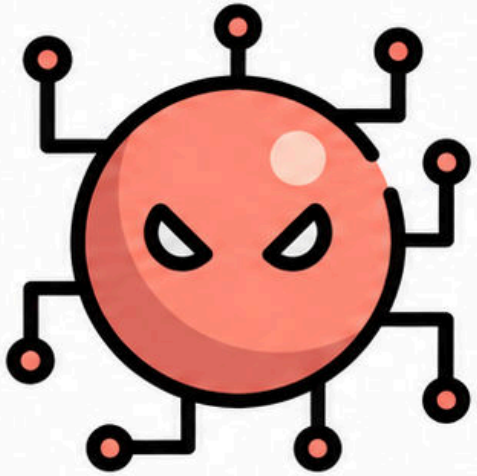
Phishing

Los ataques de phishing son los más comunes con un 83% y han aumentado un 11% en los últimos 4 años.

Ataque de intermediario

Menos del 5% de los ataques se debieron a ataques de intermediario

El **Phishing** es la práctica fraudulenta de enviar correos electrónicos que pretenden ser de empresas confiables con el fin de inducir a las personas a revelar información personal, como contraseñas y números de tarjetas de crédito. El **Malware** es un software diseñado específicamente para interrumpir, dañar o acceder de manera no autorizada a un sistema informático.



Disfrazar archivos adjuntos maliciosos como facturas falsas sigue siendo la táctica más popular para engañar a los usuarios y hacer que abran correos electrónicos de phishing y caigan en la trampa.

INTER

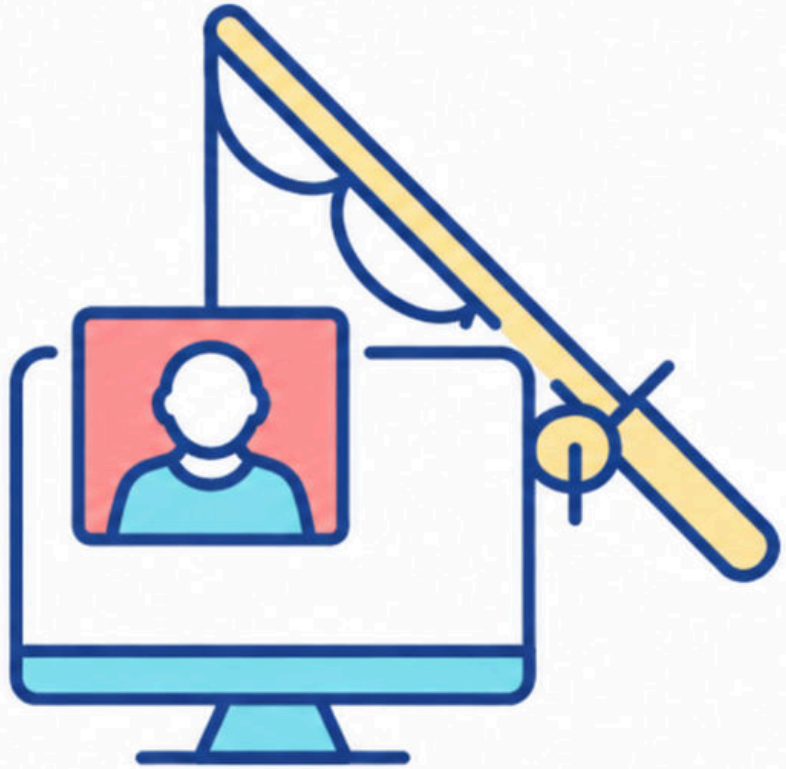
¿Cómo funciona el Phishing?

Recibes un correo electrónico o un mensaje de texto
Parece ser de alguien que conoces y te pide que hagas clic en un enlace o que proporciones tu contraseña, tu cuenta bancaria comercial u otra información confidencial.

Parece real
Es fácil falsificar logotipos e inventar direcciones de correo electrónico falsas. Los estafadores usan nombres de empresas conocidos o se hacen pasar por alguien que conoces.

Es urgente
El mensaje te presiona para que actúes ahora o algo malo sucederá.

¿Qué sucede después?
Si haces clic en un enlace, los estafadores pueden instalar ransomware u otros programas que pueden bloquear el acceso a tus datos y propagarse a toda la red de la empresa. Si compartes contraseñas, los estafadores ahora tienen acceso a todas esas cuentas.



¿Qué puedes hacer contra el Phishing?

Antes de hacer clic en un enlace o compartir información comercial confidencial:

Compruébelo

Busque el sitio web o el número de teléfono de la empresa o persona que se encuentra detrás del mensaje de texto o correo electrónico. Asegúrese de que se trata de la empresa real y no de descargar malware o hablar con un estafador.

Hable con alguien

Hablar con un colega puede ayudarlo a determinar si la solicitud es real o un intento de phishing.

Haga una llamada si no está seguro

Tome el teléfono y llame al proveedor, colega o cliente que envió el correo electrónico. Confirme que realmente necesitan información de usted. Use un número que sepa que es correcto, no el número que aparece en el correo electrónico o mensaje de texto.

INTER

Contraseñas: Qué se debe y no se debe hacer

- ✓ Utilizar la autenticación de dos factores.
- ✓ Utilizar varias palabras que no estén relacionadas.
- ✓ Utilizar una contraseña diferente para cada aplicación "elefanteazulvelagranja“.
- ✓ Utilizar un administrador de contraseñas.

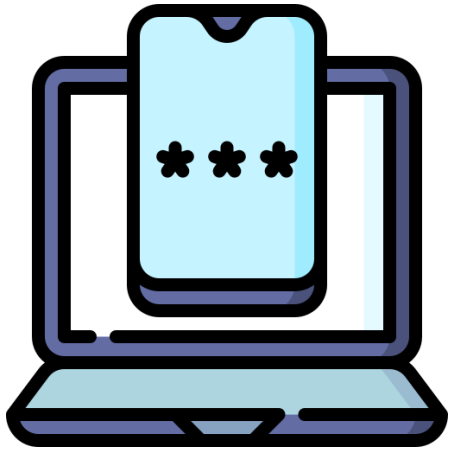
- × **NO** confiar sólo en las contraseñas.
- × **NO** contraseñas fáciles de adivinar o reutilizar.
- × **NO** crear contraseñas difíciles de recordar "&pck1s0mmz“.
- × **NO** anotar las contraseñas.

Protege tu información personal

Contraseñas seguras:

Usa contraseñas largas y complejas.

No reutilices contraseñas en diferentes sitios.



Autenticación de dos factores:

Añade una capa extra de seguridad a tus cuentas.

Cuidado con Phishing:

No abras correos electrónicos o enlaces sospechosos.

INTER

Estafas de Apoyo Técnico Falso

Recibe una llamada telefónica, una ventana emergente o un correo electrónico que le informa que hay un problema con su computadora.

A menudo, detrás de estas llamadas, mensajes emergentes y correos electrónicos se encuentran estafadores que quieren obtener su dinero, información personal o acceso a sus archivos. Esto puede dañar su red, poner en riesgo sus datos y perjudicar su negocio.

¿Qué hacer en caso de un incidente de seguridad?

Identificación:
Reconoce señales de que algo está mal (p. ej., actividad inusual en una cuenta).

Reporta:
Informa inmediatamente al equipo de Informatica de la universidad.

No entres en pánico:
Sigue los procedimientos establecidos para incidentes de seguridad.

Cómo Proteger Equipos y Archivos en Papel

Limite el acceso físico

Cuando los registros o dispositivos contengan datos confidenciales, permita el acceso solo a quienes los necesiten.

Mantenga inventario

Identifique y proteja los dispositivos que recopilan información confidencial. Conserve solo los archivos y datos que necesita y sepa quién tiene acceso a ellos.

Almacenar de forma segura

Cuando los archivos en papel o los dispositivos electrónicos contengan información confidencial, guárdelos en un armario o habitación cerrados con llave.

Enviar recordatorios

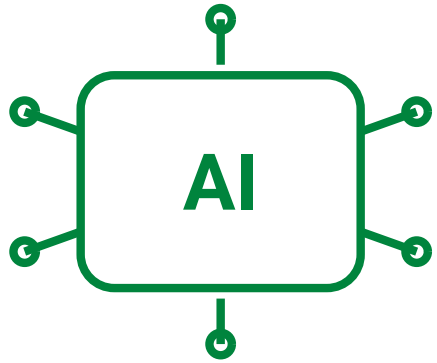
Recuerde a los empleados que guarden los archivos en papel en archivadores cerrados con llave, cierren la sesión de su red y aplicaciones, y nunca dejen archivos o dispositivos con datos confidenciales sin supervisión.

INTER

Inteligencia Artificial y Ciberseguridad

La IA también cambia el panorama de amenazas

La inteligencia artificial puede ayudar a detectar amenazas y automatizar tareas de seguridad, pero también puede facilitar fraudes, ingeniería social y contenido sintético más convincente.



Oportunidad

Usa la IA para apoyar análisis, clasificación y respuesta, siempre con supervisión humana.

Riesgo

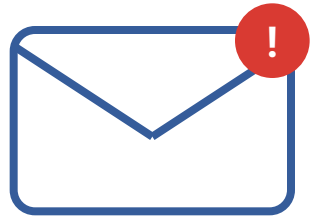
Los atacantes pueden generar mensajes, imágenes, audio y perfiles falsos a gran escala.

Regla básica: No confíes automáticamente en algo solo porque parece profesional, personalizado o “inteligente”. Verifica antes de actuar.

Phishing Potenciado por Inteligencia Artificial

¿Qué cambia con la IA?

Los mensajes fraudulentos pueden llegar con mejor redacción, contexto personalizado, nombres reales y un tono que imita a una persona o institución conocida.



Más creíble

Correos y mensajes sin errores obvios de ortografía o redacción.

Más personalizado

La información pública puede utilizarse para adaptar el engaño a ti.

Más rápido

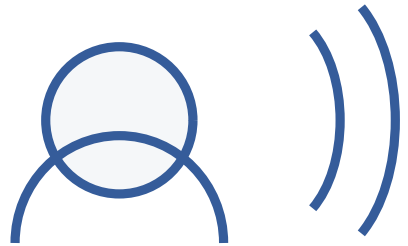
Un atacante puede producir muchas variantes del mismo fraude en poco tiempo.

Antes de responder: Verifica la dirección, el enlace y la solicitud por un canal independiente. La urgencia sigue siendo una señal de alerta.

Deepfakes y Clonación de Voz

Que una voz o un video parezcan reales no significa que lo sean.

La IA puede imitar voces, rostros y estilos de comunicación. Un atacante puede hacerse pasar por un familiar, compañero de trabajo, supervisor o figura pública para pedir dinero, credenciales o información confidencial.



Detente

No actúes por presión o urgencia.

Confirma

Contacta a la persona usando un número o canal que ya conozcas.

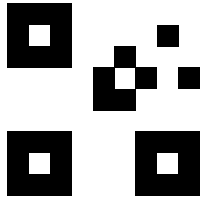
Reporta

Informa el intento si involucra cuentas, datos o recursos institucionales.

Quishing, Smishing y Vishing

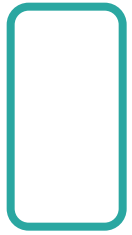
Quishing

Códigos QR que dirigen a páginas falsas para capturar credenciales o descargar contenido malicioso.



Smishing

Mensajes de texto fraudulentos que crean urgencia y solicitan abrir enlaces o compartir datos.



Vishing

Llamadas o mensajes de voz que intentan manipularte para revelar información o realizar pagos.

Antes de escanear, tocar o responder:

QR	Comprueba quién lo colocó y evita códigos inesperados en correos o documentos.
SMS	No uses el enlace del mensaje; entra al servicio desde su aplicación o sitio oficial.
Llamada	Cuelga y devuelve la llamada utilizando un número conocido.

MFA Fatigue y Autenticación Resistente al Phishing

No apruebes una solicitud MFA que no iniciaste.

En un ataque de MFA fatigue, el atacante intenta iniciar sesión repetidamente y envía múltiples notificaciones con la esperanza de que el usuario apruebe una por cansancio, confusión o error.

Si recibes una alerta

Recházala, cambia tu contraseña si sospechas compromiso y reporta el incidente.

Mejor opción

Cuando esté disponible, utiliza métodos resistentes al phishing como passkeys o llaves FIDO/WebAuthn.

Nunca compartas códigos MFA por correo, chat o teléfono.

Uso Seguro de Herramientas de Inteligencia Artificial

Antes de copiar información en una herramienta de IA, piensa en la clasificación del dato.

NO compartas

Contraseñas, tokens, números de identificación, datos financieros, expedientes o información confidencial.

SÍ verifica

Las respuestas pueden contener errores, información inventada o recomendaciones incompletas.

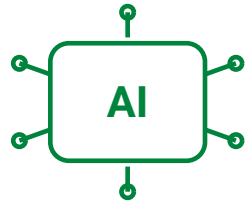
NO pegues

Documentos internos completos, información de estudiantes o empleados, ni datos que no deban salir del sistema autorizado.

SÍ utiliza

Solo herramientas y cuentas aprobadas por la institución para trabajo institucional.

Principio clave: La IA puede ayudarte a trabajar, pero no sustituye las reglas de privacidad, seguridad y manejo responsable de información.

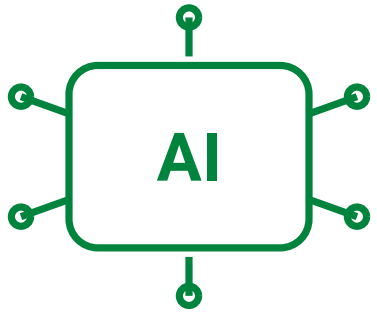


INTER

Prompt Injection y Riesgos en Agentes de IA

¿Qué es un prompt injection?

Es una técnica en la que contenido malicioso intenta cambiar las instrucciones de un sistema de IA. El riesgo aumenta cuando un agente puede leer información sensible, usar herramientas o realizar acciones.



El riesgo crece cuando una IA puede:

Leer datos

Procesar contenido externo o no confiable.

Acceder

Consultar archivos, credenciales o sistemas privados.

Actuar

Enviar mensajes, modificar datos o ejecutar acciones.

Infostealers y Robo de Sesiones

Una contraseña fuerte no siempre es suficiente si el dispositivo está comprometido.

Los infostealers son programas maliciosos diseñados para robar credenciales, cookies, tokens de sesión, datos del navegador y otra información almacenada en el equipo.

Evita software dudoso

No instales cracks, activadores, extensiones o programas de origen desconocido.

Mantén el equipo al día

Actualiza navegador, sistema operativo y herramientas de seguridad.

Si sospechas compromiso

Reporta, cambia credenciales desde un equipo seguro y cierra sesiones activas.

Señal importante: si tu navegador o cuenta se comportan de forma extraña, repórtalo antes de continuar trabajando.

INTER

Checklist de Ciberseguridad 2026

Piensa antes de hacer clic

Verifica enlaces, adjuntos, QR y solicitudes inesperadas.

Desconfía de la urgencia

Una voz, video o mensaje convincente también puede ser falso.

Protege tus cuentas

Usa contraseñas únicas, administrador de contraseñas y MFA.

Usa la IA con responsabilidad

No compartas datos confidenciales y verifica sus respuestas.

Actualiza

Mantén sistema, navegador y aplicaciones al día.

Reporta

Si algo parece extraño, informa de inmediato al equipo de Informática.

La seguridad cibernética es una responsabilidad compartida. Detente, verifica y reporta antes de que un incidente se convierta en un problema mayor.

INTER