	<b>NOMBRE DEL PROCEDIMIENTO</b>  <b>CORREO SOSPECHOSO, EMPRESA SEGURA</b>		Código SOPORTE-TI-0001
			Versión: 0.2
Elaboró Analista I + D + i	Aprobó	Revisó	
Fecha 05/08/2025	Fecha	Fecha	

**Nombre de la campaña:** “Correo Sospechoso, Empresa Segura”

**Dirigida a:** Empleados que participaron en simulaciones de phishing o ingeniería social

**Objetivo:** Fortalecer la cultura de ciberseguridad en la empresa mediante una campaña educativa dirigida a los empleados que participaron en simulaciones de ataques controlados, como phishing y llamadas de ingeniería social. Esta campaña busca no solo explicar el propósito de las pruebas de pentesting interno, sino también brindar conocimientos prácticos y recomendaciones claras para que cada colaborador pueda actuar de manera segura, consciente y proactiva ante amenazas digitales reales, reduciendo así el riesgo humano como vector de ataque.

#### **Módulo 1: ¿Qué es la Ciberseguridad?**

La ciberseguridad es el conjunto de prácticas, tecnologías y procesos diseñados para proteger los sistemas informáticos, redes, dispositivos y datos contra ataques digitales y accesos no autorizados. Implica proteger información sensible y activos digitales, prevenir y responder a ciberataques, y garantizar la integridad y disponibilidad de sistemas y redes. la ciberseguridad busca:

- **Proteger la información:**  
Evitar el acceso no autorizado, la modificación o destrucción de datos confidenciales.
- **Prevenir ataques:**  
Implementar medidas para reducir la vulnerabilidad a ataques y evitar que ocurran.
- **Responder a incidentes:**  
Desarrollar planes y procedimientos para hacer frente a ataques exitosos y minimizar su impacto.
- **Mantener la continuidad del negocio:**  
Asegurar que las operaciones puedan continuar incluso después de un incidente de seguridad.

La ciberseguridad es importante porque:

- La dependencia de la tecnología digital aumenta:

Las organizaciones y personas dependen cada vez más de sistemas y redes para realizar sus operaciones y almacenar información.

- Los ciberataques son cada vez más sofisticados:

Los atacantes utilizan técnicas avanzadas para explotar vulnerabilidades y causar daños.

- Las consecuencias de un ataque pueden ser graves:

Pueden incluir pérdida de datos, interrupción del negocio, daños a la reputación y pérdidas financieras.

Algunos ejemplos de áreas cubiertas por la ciberseguridad incluyen:

- Seguridad de la red:

Protección de la infraestructura de red, como firewalls, sistemas de detección de intrusiones y protocolos de seguridad.

- Seguridad de la información:

Protección de datos confidenciales, incluyendo la implementación de políticas de acceso, cifrado y gestión de identidades.

- Seguridad en la nube:

Protección de sistemas y datos almacenados en la nube, utilizando soluciones de seguridad específicas para entornos cloud.

- Seguridad de aplicaciones:

Protección de aplicaciones web y móviles contra vulnerabilidades y ataques.

- Seguridad física:

Protección de los sistemas y centros de datos contra accesos no autorizados o daños físicos.

En resumen, la ciberseguridad es esencial para proteger la información, los sistemas y la reputación en la era digital. Implica una combinación de tecnología, procesos y capacitación para garantizar que las organizaciones y las personas estén protegidas contra las amenazas cibernéticas.

### **Tipos de amenazas comunes:**

#### **Phishing:**

El phishing es una técnica de ciberataque que busca engañar a las personas para que revelen información personal confidencial, como contraseñas, números de tarjetas de crédito o datos bancarios. Los atacantes suelen hacerse pasar por entidades legítimas, como bancos o redes sociales, a través de correos electrónicos, mensajes de texto o sitios web fraudulentos.

¿Cómo funciona?

El phishing se basa en la ingeniería social, manipulando a las víctimas para que divulguen sus datos. Los atacantes pueden:

- Enviar correos electrónicos o mensajes de texto que parecen provenir de fuentes confiables:

Estos mensajes suelen incluir enlaces que dirigen a páginas web falsas que imitan a las originales.

- Solicitar información personal o financiera:

Los mensajes pueden pedir que se verifique la cuenta, se actualicen los datos o se reclame un premio, utilizando un lenguaje urgente para generar presión.

- Incluir archivos adjuntos maliciosos:

Estos archivos pueden contener malware que infecta el dispositivo de la víctima al abrirllos.

¿Cómo protegerse del phishing?

- Desconfiar de mensajes sospechosos: Prestar atención a errores gramaticales, saludos genéricos y solicitudes urgentes de información personal.
- Verificar la URL del sitio web: Asegurarse de que la dirección web sea la correcta y no una versión falsa.
- No hacer clic en enlaces sospechosos: Ingresar directamente a los sitios web a través de la barra de direcciones del navegador.
- No proporcionar información personal por correo electrónico o mensajes de texto: Contactar directamente con la entidad a través de canales oficiales si se tiene alguna duda.
- Mantener el software actualizado: Esto incluye el sistema operativo, el navegador web y el antivirus.
- Usar contraseñas seguras y autenticación de doble factor: Esto dificulta el acceso a las cuentas incluso si se filtran las contraseñas.

**Tipos de phishing:**

- Phishing por correo electrónico: El tipo más común, donde los atacantes envían correos electrónicos fraudulentos.
- Spear phishing: Ataques dirigidos a personas específicas, a menudo ejecutivos de alto nivel.
- Smishing: Ataques a través de mensajes de texto.
- Vishing: Ataques que utilizan llamadas telefónicas.

BEC (Compromiso del correo electrónico empresarial): Ataques dirigidos a empresas para robar información valiosa.

**Malware**

El malware es software malicioso diseñado para infiltrarse en sistemas informáticos con el objetivo de dañarlos, interrumpirlos o acceder a ellos de forma no autorizada. Los ciberdelincuentes lo utilizan para robar información, obtener acceso a credenciales bancarias, vender acceso a recursos informáticos o información personal, o extorsionar a las víctimas.

**Tipos de malware:**

- Virus: Se adjuntan a archivos o programas y se propagan cuando se ejecutan esos archivos.

- Gusanos: Se propagan por sí mismos a través de redes, sin necesidad de la acción del usuario.
- Troyanos: Se presentan como software legítimo para engañar al usuario y ocultar su función maliciosa.
- Spyware: Recopila información confidencial del usuario de forma encubierta, como contraseñas y datos bancarios.
- Adware: Muestra anuncios intrusivos y puede recopilar datos del usuario.
- Ransomware: Cifra los archivos de la víctima y exige un rescate para descifrarlos.

### **Cómo protegerse del malware:**

- Mantener el software actualizado: Las actualizaciones suelen incluir parches de seguridad que corrigen vulnerabilidades.
- Usar un software antivirus y antimalware: Estas herramientas pueden detectar y eliminar software malicioso.
- Tener precaución con los correos electrónicos y enlaces sospechosos: No abrir archivos adjuntos ni hacer clic en enlaces de remitentes desconocidos.
- Descargar software solo de fuentes confiables: Evitar descargar programas de sitios web desconocidos o poco seguros.
- Hacer copias de seguridad regularmente: En caso de infección por ransomware, tener copias de seguridad de los archivos importantes puede ser crucial.

### **Ransomware**

El ransomware es un tipo de malware (software malicioso) que restringe el acceso a archivos o sistemas, generalmente mediante el cifrado, hasta que se paga un rescate. Los atacantes amenazan con mantener los datos bloqueados o incluso eliminarlos si no se paga el rescate. Los ataques de ransomware pueden causar graves interrupciones en las operaciones y la pérdida de datos valiosos.

- **Cómo funciona:**

El ransomware puede propagarse a través de enlaces o archivos adjuntos maliciosos, ataques de phishing, o explotando vulnerabilidades en software. Una vez que infecta un sistema, puede cifrar archivos, bloquear el acceso al sistema o incluso robar datos.

- **Tipos de ransomware:**

Existen diferentes tipos, como el ransomware de cifrado, que cifra los archivos, y el ransomware de bloqueo de pantalla, que bloquea la pantalla del dispositivo.

- **Pagos de rescate:**

Los atacantes suelen exigir el pago de un rescate en criptomonedas, como Bitcoin, para liberar los datos o el sistema. Es importante destacar que no hay garantía de que los atacantes cumplan con su parte del trato después de recibir el pago.

- **Impacto:**

Los ataques de ransomware pueden afectar a individuos, empresas y organizaciones de todos los tamaños, causando interrupciones en las operaciones, pérdida de datos y daños a la reputación.

- **Prevención:**

Para protegerse contra el ransomware, es crucial tener copias de seguridad actualizadas de los datos, mantener el software actualizado, utilizar contraseñas seguras, tener cuidado con los enlaces y archivos adjuntos sospechosos, y usar software antivirus y antimalware confiable.

## **Ingeniería social**

La ingeniería social, en el contexto de la seguridad informática, se refiere a la práctica de manipular a las personas para que realicen acciones que comprometan la seguridad de sistemas, redes o información confidencial. Los atacantes, utilizando técnicas de engaño y manipulación, se aprovechan de la confianza y vulnerabilidades psicológicas de las personas para obtener acceso a datos o sistemas.

En resumen, la ingeniería social no se trata de ataques técnicos, sino de ataques psicológicos que explotan la naturaleza humana para lograr sus objetivos.

¿Cómo funciona?

- **Manipulación:**

Los atacantes se hacen pasar por personas o entidades de confianza, como compañeros de trabajo, soporte técnico o incluso amigos, para ganarse la confianza de la víctima.

- **Engaño:**

Utilizan pretextos, historias falsas y situaciones manipuladas para convencer a la víctima de que realice ciertas acciones, como divulgar contraseñas, instalar software malicioso o acceder a sitios web fraudulentos.

- **Explotación de la confianza:**

La ingeniería social se basa en la tendencia humana a confiar en los demás y a seguir instrucciones de figuras de autoridad, lo que la convierte en una técnica efectiva para eludir las medidas de seguridad técnicas.

Ejemplos de ataques de ingeniería social:

- **Phishing:**

Envío de correos electrónicos o mensajes que parecen provenir de fuentes legítimas, solicitando información confidencial o credenciales de acceso.

- **Tailgating:**

Seguir a una persona autorizada a una zona restringida, aprovechando su cortesía para obtener acceso.



- Pretextos:

Inventar una historia convincente para engañar a la víctima y obtener información.

- Ataques de cebo:

Dejar dispositivos infectados en lugares públicos para que alguien los recoja y los utilice, propagando malware.

- Educación y concienciación:

Informar a los usuarios sobre las técnicas de ingeniería social y cómo identificarlas.

- Verificación:

Desconfiar de solicitudes inusuales o inesperadas, y verificar la autenticidad de la fuente.

- Contraseñas seguras:

Utilizar contraseñas complejas y únicas, y no compartirlas con nadie.

- Software de seguridad:

Mantener el software de seguridad actualizado y realizar análisis periódicos.

Al comprender las técnicas de ingeniería social y tomar medidas preventivas, podemos reducir significativamente el riesgo de ser víctimas de este tipo de ataques.

¿Por qué importa?

- Porque la seguridad digital ya no es solo un tema técnico, es una responsabilidad de todos.

Un solo clic en un enlace malicioso, una contraseña compartida o una llamada mal atendida pueden ser suficientes para:

- Exponer información confidencial de la empresa y de nuestros clientes.
- Interrumpir operaciones críticas, afectando productividad, logística y finanzas.
- Poner en riesgo la reputación de la empresa, generando desconfianza en aliados y proveedores.
- Convertirnos en una puerta de entrada para ciberdelincuentes que buscan robar, extorsionar o manipular datos.

La ciberseguridad empieza por nuestro comportamiento diario. Cada decisión que tomamos frente a un correo, un archivo o una llamada, suma o resta a la protección de toda la organización.

## **Módulo 2: ¿Qué es un Pentesting Interno?**

Simulación de ataques éticos dentro de la empresa.

Permite encontrar debilidades antes de que los atacantes reales lo hagan.

## **Beneficios:**

- Concientización del personal.
- Mejora de políticas internas.
- Reducción de riesgo reputacional y financiero.

## **Módulo 3: ¿Qué pasó en la simulación de phishing?**

- Explicación al empleado:  
Se le envió un correo falso como parte de un ejercicio controlado.
- Hacer clic o ingresar datos demuestra una vulnerabilidad explotable.
- No se recolectaron contraseñas reales ni se comprometió su seguridad personal.

## **Módulo 4: ¿Qué ocurrió con la llamada telefónica falsa?**

Explicación al empleado:

- Fue una prueba ética de ingeniería social.
- Se midió si el empleado verifica la identidad del interlocutor antes de entregar datos.

## **Módulo 5: ¿Cómo actuar ante estas situaciones?**

Recomendaciones claras:

Ante un correo sospechoso:

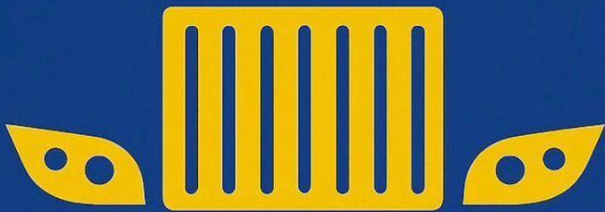
- 1.No hagas clic.
- 2.No descargues archivos adjuntos.
- 3.Verifica con el remitente por otro canal.
- 4.Reenvía a TIC para revisión.

Ante una llamada dudosa:

- 1.Pregunta nombre completo, cargo y extensión interna.
- 2.Nunca entregues credenciales por teléfono.
- 3.Reporta la llamada al equipo TIC.

General:



1. Usa contraseñas seguras y cámbialas regularmente.
2. Bloquea tu equipo cuando te ausentes.
3. No compartas información interna por WhatsApp personal o redes sociales.



## SIMÓN BOLÍVAR

Todo para vehículos pesados

# 10 señales de un correo malicioso

 <b>Símbolos extraños en el correo</b>	 <b>Sentido de urgencia</b>
 <b>Solicitudes inesperadas</b>	 <b>Errores gramaticales</b>
 <b>Falta de información de contacto</b>	 <b>Correos electrónicos sospechosos</b>
 <b>Enlaces sospechosos</b>	 <b>Documentos adjuntos sospechosos</b>
 <b>Enlace a dominios que no coinciden</b>	 <b>No coincide con ningún correo anterior</b>



### **Evaluación de Retroalimentación:**

Ingresa en el siguiente link y llena el formulario:

<https://forms.office.com/Pages/ResponsePage.aspx?id=u1m05b49mUmlLsvxzt2xZuuLln2c8WNJjQsCv4lQg1lUOUNMTDBXNzBBQ1lKOU1GTVBNSFc0T1Y3Ny4u>

### **Relación**

- Pentesting Humano.

