



Escuela Tecnológica Instituto Técnico Central  
Establecimiento Público de Educación Superior

# Seguridad Digital

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI

 <p><b>DUMPSTER DIVING</b> Explorar información ubicada en la basura, aprovechando el descuido de los individuos que arrojan documentos con información confidencial sin haberlos destruido.</p>	 <p><b>SEXTORSIÓN</b> Técnica donde se amenaza a la víctima para no publicar imágenes comprometedoras a cambio de dinero.</p>	 <p><b>PHISHING</b> Este tipo de ataque se basa en la suplantación de identidad, casi siempre por enlaces maliciosos por correo electrónico.</p>	 <p><b>PRETEXTINTING</b> El atacante intenta convencer a una víctima para que renuncie a información valiosa, así como el acceso a un servicio o sistema.</p>
 <p><b>SHOULDER SURFING</b> Espiar por encima del hombro de las personas para observar lo que están tecleando y así poder obtener contraseñas, PIN o patrones de desbloqueo.</p>	 <p><b>BAITING</b> Usa un medio físico como discos o USB en lugares de confianza para atraer la atención de la víctima con el fin de conectarlos en los dispositivos y capturar su información.</p>	 <p><b>SMISHING</b> Envío de mensajes de texto (SMS) con enlaces maliciosos para obtener información confidencial.</p>	 <p><b>SPEAR PHISHING</b> Estafa de correo electrónico o comunicaciones dirigida a personas, organizaciones o empresas específicas.</p>

Escuela Tecnológica Instituto Técnico Central

## PHISHING SIGNIFICA

engañar a alguien para que haga clic en un enlace y recopilar así su información confidencial como números de tarjetas de crédito y contraseñas.

**NO HAGAS CLIC: CÚIDATE DEL PHISHING**



Escuela Tecnológica Instituto Técnico Central

## NO HAGAS CLIC: CÚIDATE DEL PHISHING

- Abre correos electrónicos de personas que conoces
- Si algo se ve mal, pregúntale a la persona si en verdad lo envió
- No hagas clic en los enlaces
- Antes de abrir un archivo adjunto, revisa que no tenga virus



 <p>Los ciberdelincuentes no siempre buscan un lucro económico. También hay factores como la notoriedad, superación propia e incluso pérdida de reputación de la compañía atacada.</p>	 <p>Al hablar de hacking ético se hace referencia a los hackers de sombrero blanco, que luchan por detectar vulnerabilidades en los sistemas para mejorar la seguridad de estos.</p>
 <p>Concientizan a la alta dirección de la importancia de apostar por la seguridad de la información a través de los resultados obtenidos en el hacking.</p>	 <p>Mejoran los procesos existentes y la seguridad de los sistemas en la compañía para disponer de un plan eficaz de gestión de incidencias.</p>

El *hacking* ético es una de las especialidades en ciberseguridad más demandadas por las empresas.

Con este, se pueden defender detectando y mitigando vulnerabilidades existentes en los sistemas y plataformas de tecnología que pueden ser explotadas por los delincuentes.

## ¡PROTEJA SU PRIVACIDAD CON CONTRASEÑAS SEGURAS!

- Utilice mínimo 6 caracteres alfanuméricos
- Incluya letras mayúsculas, minúsculas, números y símbolos

Tome como referencia el siguiente ejemplo:

**"eT7mPr2!"**

Recuérdelo con una frase:

"ella TENÍA 7 manzanas PERO regaló 2!"

Escuela Tecnológica Instituto Técnico Central

## ¿AÚN NO TIENES TU CARNE DIGITAL?

Este mes de agosto asiste a la toma de tu fotografía en el Auditorio ETITC Centro.

<b>MARTES 9</b>	DE 5:00 A 8:00 P. M.
<b>JUEVES 11</b>	DE 3:00 A 6:00 P. M.
<b>MARTES 16</b>	DE 5:00 A 8:00 P. M.
<b>JUEVES 18</b>	DE 3:00 A 8:00 P. M.

\*Si eres estudiante debes estar matriculado  
\*Si eres docente o administrativo y aún no tienes carné, también te esperamos



PARA ALGUNA AYUDA:



 seguridaddigital@itc.edu.co

 Ingeniera. Sandra Guerrero