POSITIVA COMPAÑÍA DE SEGUROS | suma 5.0 | educa | comunica

EL FUTURO ES HUMANO

PLAN NACIONAL

Multimodal 2025

Fórmulas para la vida

Valores + Emociones + Competencias

Respeto + Alegría + Aprendizaje

10

POSITIVA COMPAÑÍA DE SEGUROS | suma 5.0 | educa | comunica

EL FUTURO ES HUMANO

Comunidad Nacional de Conocimiento para

La Prevención de Riesgos Públicos

Fórmulas para la vida

Valores + Emociones + Competencias

Responsabilidad+ Gratitud + Resiliencia

SESIÓN 6:
ANÁLISIS DE LA MATERIALIZACIÓN DE LA ESTAFA Y CIBER DELITO

PAOLA ANDREA RAMIREZ AVILA

COMUNIDAD NACIONAL DE CONOCIMIENTO PARA LA PREVENCIÓN DE RIESGOS PÚBLICOS

Pararamirez@hotmail.com

3142053053

ADMINISTRADORA DE EMPRESAS, ESPECIALISTA EN DOCENCIA UNIVERSITARIA, Y EN GESTIÓN DEL TALENTO HUMANO; MAGISTER EN DIRECCIÓN DE PERSONAL Y EN SEGURIDAD Y SALUD EN EL TRABAJO. COACH ONTOLÓGICO, TUTOR VIRTUAL DE DIFERENTES UNIVERSIDADES, CONFERENCISTA DE LA CÁMARA INTERNACIONAL DE CONFERENCISTAS. ASESORA Y CONSULTORA EN RIESGOS LABORALES, DESARROLLO HUMANO Y SISTEMAS INTEGRADOS DE GESTIÓN.
(CEO) PROHUMANA SOLUCIONES.

Ruta de **conocimiento**

SESIÓN 1:
PREVENCIÓN DE LA EXTORSIÓN A PERSONAS Y ENTIDADES

SESIÓN 2:
PREVENCIÓN FRENTE AL RETEN ILEGAL - PESCA MILAGROSA

SESIÓN 3:
GESTIÓN DEL RIESGO EN COMISIONES Y AUTORIZACIONES DE TRABAJO EN LAS REGIONES

SESIÓN 4:
PREVENCIÓN DEL RIESGO EN MANIFESTACIÓN PÚBLICA QUE SE VUELVE ASONADA

SESIÓN 5:
PREVENCIÓN DEL RIESGO PÚBLICO - ATRACO

Ruta de **conocimiento**

SESIÓN 6:
ANÁLISIS DE LA MATERIALIZACIÓN DE LA ESTAFA Y CIBER DELITO

SESIÓN 7:
PREVENCIÓN DEL SECUESTRO

SESIÓN 8:
PREVENCIÓN DEL RIESGO PÚBLICO - IDENTIFICACIÓN DE PAQUETES EXPLOSIVOS

SESIÓN 9:
PREVENCIÓN DEL RIESGO PÚBLICO - TIPOS DE ESTAFA

SESIÓN 10:
PREVENCIÓN DEL RIESGO PÚBLICO - RECONOCIMIENTO DEL DELITO EN COLOMBIA


POSITIVA
COMPAÑÍA DE SEGUROS
suma 5.0
educa
comunica
EVALUÉMONOS
Fórmulas para la vida
Valores + Emociones + Competencias
Respeto + Gratitud + Ética y sostenibilidad


"La seguridad no es un producto, sino un proceso."
(Bruce Schneier)

CONTENIDO

OBJETIVOS

01 Socializar los conceptos de riesgo público que se pueden materializar de acuerdo a los riesgos laborales

02 Reconocer la estafa, como una modalidad vigente en riesgo público nacional

03 Reconocer los tipos de ciberdelitos y las herramientas de prevención en los entornos laborales y de alcance personal

RIESGO PÚBLICO

Es la posibilidad de que, durante el ejercicio de la actividad laboral, por fuente, situación o acto, los trabajadores puedan verse afectados en su integridad física o mental, derivado de una acción antrópica intencional; asimismo, incluye la afectación de bienes (tecnológicos, sistemas, muebles e inmuebles y medio ambiente).

Configuración del Agente Generador del Peligro

Oportunidad

- Desconocimiento
- Falta de antivirus
- Vulnerabilidad informática

Motivo

- Imprudencia
- Curiosidad
- Ambición

Motivo

- Económico
- Personales
- Laborales

Materialización Riesgo Publico

DEFINICIÓN LEGAL Y MARCO NORMATIVO
ESTAFA

En Colombia, la estafa está tipificada en el Artículo 246 del Código Penal (Ley 599 de 2000), a la letra dice:

"El que obtenga provecho ilícito para sí o para un tercero, con perjuicio ajeno, induciendo o manteniendo a otro en error por medio de artificios o engaños …"

CARACTERÍSTICAS PRINCIPALES DE LA ESTAFA

Engaño o artificio

- El autor usa maniobras fraudulentas, trucos, falsedades, simulaciones o cualquier medio que induzca a error a la víctima.
- El engaño debe ser suficiente para convencer a una persona promedio en esas circunstancias.

Inducción o mantenimiento en error

- La víctima, debido al engaño, cree en una falsa representación de la realidad.
- Puede ser inducida inicialmente al error o mantenida en él durante cierto tiempo.

Acto de disposición patrimonial de la víctima

- La persona engañada realiza voluntariamente un acto de disposición (ej. entregar dinero, firmar un contrato, transferir un bien).
- Este acto es clave: si no hay disposición patrimonial, no hay estafa.

Perjuicio Ajeno

- Correlativamente, la víctima o un tercero sufre un daño patrimonial.
- La estafa siempre implica beneficio para uno y pérdida para otro.

Dolo directo (intención fraudulenta)

- El autor actúa con intención clara de engañar y lucrarse.
- No basta un simple incumplimiento de contrato: debe haber fraude desde el inicio.

Bien jurídico protegido

- Lo que protege la norma es la propiedad y el patrimonio económico de las personas.

Obtención de provecho ilícito

- El autor o un tercero obtiene un beneficio económico indebido, fruto del engaño.
- Ese beneficio puede ser dinero, bienes, servicios, derechos o ventajas patrimoniales.

Tipos de estafa

Algunas de las modalidades más frecuentemente reportadas en Colombia en los últimos años:

Modalidad	Descripción / Cómo operan
Phishing / Suplantación de entidades oficiales	Correos electrónicos, mensajes de texto o llamadas haciéndose pasar por bancos, entidades como la DIAN, EPS, etc., para obtener datos sensibles o dinero.
Falsos enlaces de ofertas / Marketplace engañoso	Promesas de productos baratos, ofertas laborales, servicios que piden primero un pago o datos, pero no entregan nada.
WhatsApp clonado / cuenta comprometida	Roban o clonan cuentas de usuarios y piden dinero a sus contactos haciéndose pasar por ellos.
Estafas relacionadas con multas de tránsito falsas u otros avisos oficiales falsos	Mensajes que alertan sobre multas inexistentes con enlaces fraudulentos para "resolver" la multa.
Esquemas piramidales / captación ilegal de dinero	Prometen retornos altos, rápidos, sin respaldo; muchas veces funcionan como Ponzi; han sido casos muy grandes en Colombia.

DELITOS INFORMÁTICOS SEGÚN LA LEY 1273 DE 2009

ARTÍCULO	CONDUCTA
269A – Acceso abusivo a un sistema informático	Entrar, permanecer o usar un sistema informático sin autorización o excediendo permisos.
269B – Obstaculización ilegítima de sistema informático o red de telecomunicación	Interferir, obstaculizar o afectar el funcionamiento de un sistema informático o red.
269C – Interceptación de datos informáticos	Interceptar datos informáticos en transmisión sin autorización.
269D – Daño informático	Borrar, deteriorar, alterar o suprimir datos informáticos o programas sin autorización.
269E – Uso de software malicioso	Producir, traficar, usar o facilitar programas diseñados para afectar sistemas informáticos (virus, troyanos, malware).
269F – Violación de datos personales	Obtener, transferir, modificar o usar datos personales sin autorización.
269G – Suplantación de sitios web para capturar datos personales	Crear, divulgar o usar sitios web falsos para captar datos (ej: phishing).
269H – Circunstancias de agravación punitiva	Agrava la pena si: la conducta afecta información de carácter público, de entidades financieras, de seguridad del Estado, o si se causa grave perjuicio económico.
269I – Hurto por medios informáticos y semejantes	Apoderarse de bienes ajenos transfiriendo dinero u otros activos mediante manipulación informática.
269J – Transferencia no consentida de activos	Transferir sin autorización fondos o valores usando medios electrónicos o informáticos.


FRAUD ALERT
DELITOS
INFORMÁTICOS

IA

Inteligencia artificial que permite crear imágenes, campañas, voz, e información para deteriorar la imagen o crear conflictos amenazantes.

CIBERSEGURIDAD

Conocida como cualquier situación en la que se utilicen indebidamente datos y / o información personal a través de la red o el mundo virtual, para cometer delitos, provocando pérdidas a las víctimas, que pueden ser tanto personas como empresas.

Ciber extorsión o (Sexting)

Es un delito cometido por delincuentes a través de plataformas virtuales, los niños, niñas y adolescentes pueden ser víctimas de engaños en internet con el fin de conseguir fotos, videos, en su mayoría íntimos con el fin de más adelante contactar a las víctimas creando una falsa amistad y luego poder chantajearlos pidiendo altas sumas de dinero a cambio de no publicar las fotos o videos que fueron enviados.

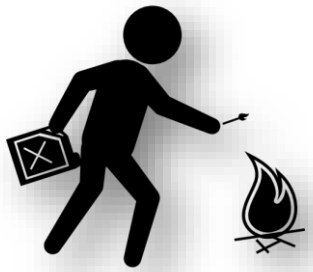
Extorsión con fotos intimas

Que hacer si me están extorsionando con fotos?.

1. Cuéntaselo a alguien de confianza.

2. Evita todo contacto con el ciber criminal

3. No borre nada y tome evidencias.



4. Realice una denuncia ante las autoridades.

5. Reporte la cuenta del ciber criminal.

“ Recuerde que la mejor manera de evitar la sextorsión, es no enviando contenido intimo.”

Extorsiones en plataformas virtuales

¿cómo prevenirla?

- En las redes sociales no se debe exponer la vida íntima. Cuando una fotografía, vídeo o información de carácter personal es publicada, se pierde su control y los ciberdelincuentes pueden aprovechar lo compartido para hacer daño.
- Al buscar información en Internet es aconsejable verificar el protocolo de seguridad https para comprobar que se está visitando un sitio web seguro.
- La descarga de aplicativos en dispositivos siempre tiene que realizarse desde páginas oficiales.
- No acceder a sitios web a través de enlaces de dudosa procedencia. Lo mejor es visitarlos mediante buscadores oficiales.
- Finalmente, la Policía Nacional de Colombia insta a los padres de familia a vigilar los hábitos de sus hijos: lugares que frecuentan, conocer a sus amistades, observar cambios de comportamiento, etc.

Delito patrimonial

Es un delito patrimonial consistente en emplear el engaño con ánimo de lucro para provocar un error en la víctima, induciéndola a realizar un acto de disposición en perjuicio de sí misma o de un tercero.

Este delito puede ser cometido sobre bienes muebles, bienes inmuebles, derechos y servicios.

El principal bien jurídico protegido en el delito de estafa es el patrimonio, considerándose también protegidos la buena fe y las relaciones de confianza.

El tipo básico del delito de estafa se regula en el artículo 248 del Código Penal, y el artículo 249

Recoge supuestos específicos de este delito. El delito de estafa está sancionado con una pena de prisión de **6** meses a **3** años.

PHISHING

(Suplantación de identidad)

Es un método en el cual los delincuentes se hacen pasar por conocidos de las personas, plataformas de e-commerce o instituciones financieras para robar datos personales y bancarios de sus víctimas.

La estafa consiste en crear un sitio web falso extremadamente similar al de algunas empresas legítimas. A través de mensajes vía correo electrónico, Whatsapp o SMS, los delincuentes envían un enlace, solicitando la confirmación de los datos. Al hacer clic en este enlace, las víctimas son redirigidas al sitio web falso, donde terminan cayendo en la trampa y proporcionando sus datos.

Aprende a identificar EL PHISHING

1. La mayoría de estos correos tienen errores de escritura bastante notables.
2. La pagina web haca donde lo dirigen para que ingrese sus datos no coinciden con la pagina autentica de la entidad.
3. El objetivo de phishing siempre sea obtener información, por lo que le pueden pedir:

➢ Usuarios y contraseñas

➢ Números de tarjetas de crédito

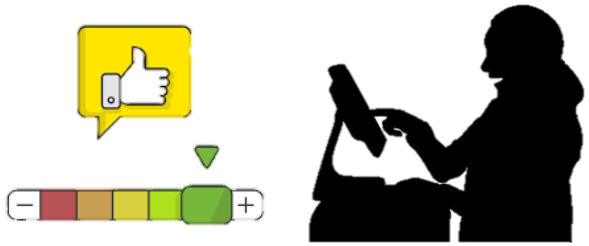
➢ Numero de cuentas bancarias

Recuerde que ninguna entidad bancaria te solicitar estos datos por correo electrónico.

Recomendaciones para comprar seguro en internet

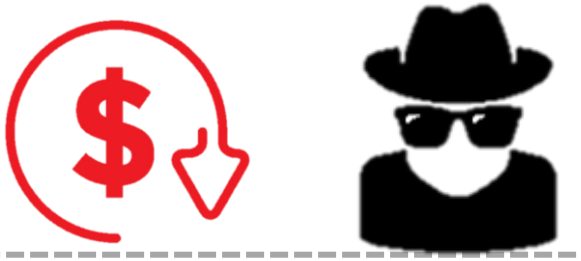
En 3 simples pasos…

1. Verifique la identidad del vendedor y su reputación antes de realizar la transacción.



2. En lo posible utilice únicamente plataformas verificadas que brinden respaldo en caso de un problema con el vendedor.

3. Sospeche siempre de ofertas con precios demasiado bajos y compare con otras tiendas o vendedores.



“ Recuerde que la mejor manera de evitar la estafas, es visitar las paginas oficiales y de confianza.”

Estafas de servicio al cliente

¿Como funciona?

El cibercriminal crea una cuenta falsa suplantando la imagen de la entidad para atraer victimas.

¿Cuál es su objetivo?

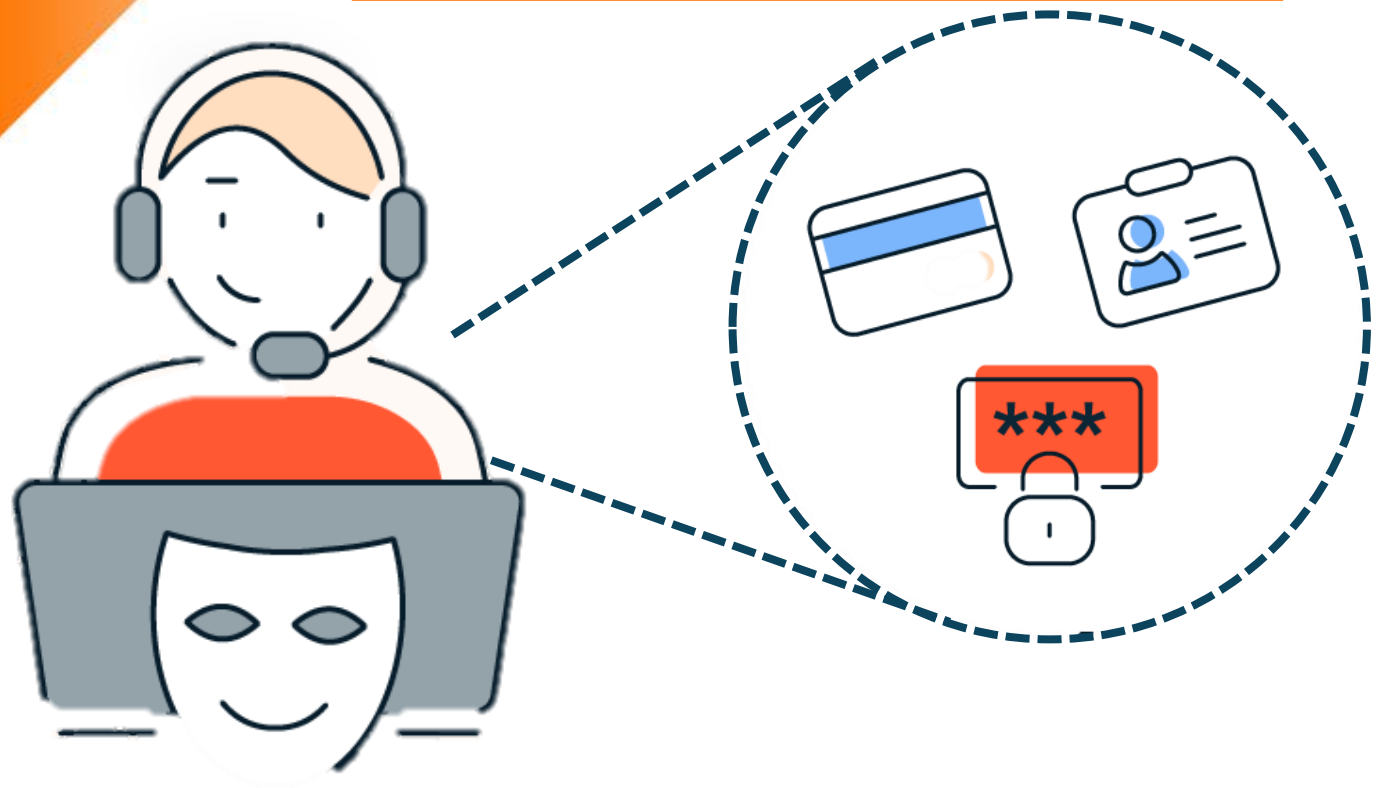
Que la victima suministre datos sensibles o descargue algunas aplicaciones maliciosas en sus dispositivos.

¿CÓMO PROTEGERSE?

¿Cómo evitarlo?

Siempre verifique que la información de la cuenta, coincida con los datos en otros canales oficiales de la entidad.

EL VISHING



En que consiste ?

Conocido como **phishing telefónico**, en donde los delincuentes simulan ser empleados de alguna institución y generalmente te convencen al decirte que tus cuentas están registrando cargos irregulares o que requieren alguna información, evita proporcionarles tus datos y llama directamente a la institución financiera para corroborar la información.

EL VISHING

Aprende a identificarlo

1. Le piden confirmar datos de su tarjeta de crédito o debito como :

* Código de seguridad

* Numero de la tarjeta

* Fecha de vencimiento

Las entidades bancarias nunca le solicitaran información sensible sobre sus cuenta. Estas son algunas señales que le deben alertar:

2. Datos personales que la entidad conoce como:

- Dirección de residencia.

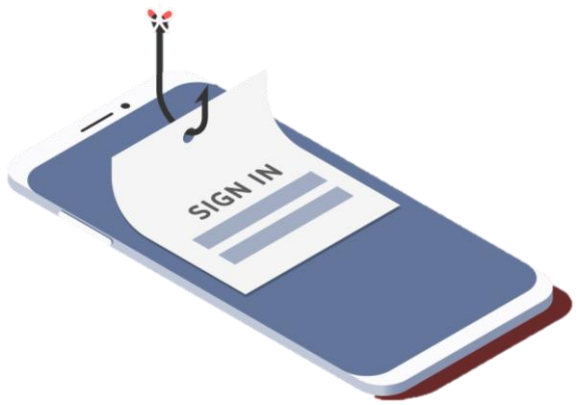
- Numero de cedula.

- Correos electrónicos.

SMISHING

Suplantación de identidad

Un ataque de smishing es un tipo de ataque de phishing que aprovecha **los mensajes de texto como vector de ataque**. Puede basarse en ingeniería social, archivos adjuntos maliciosos y sitios web fraudulentos para estafar a la gente.



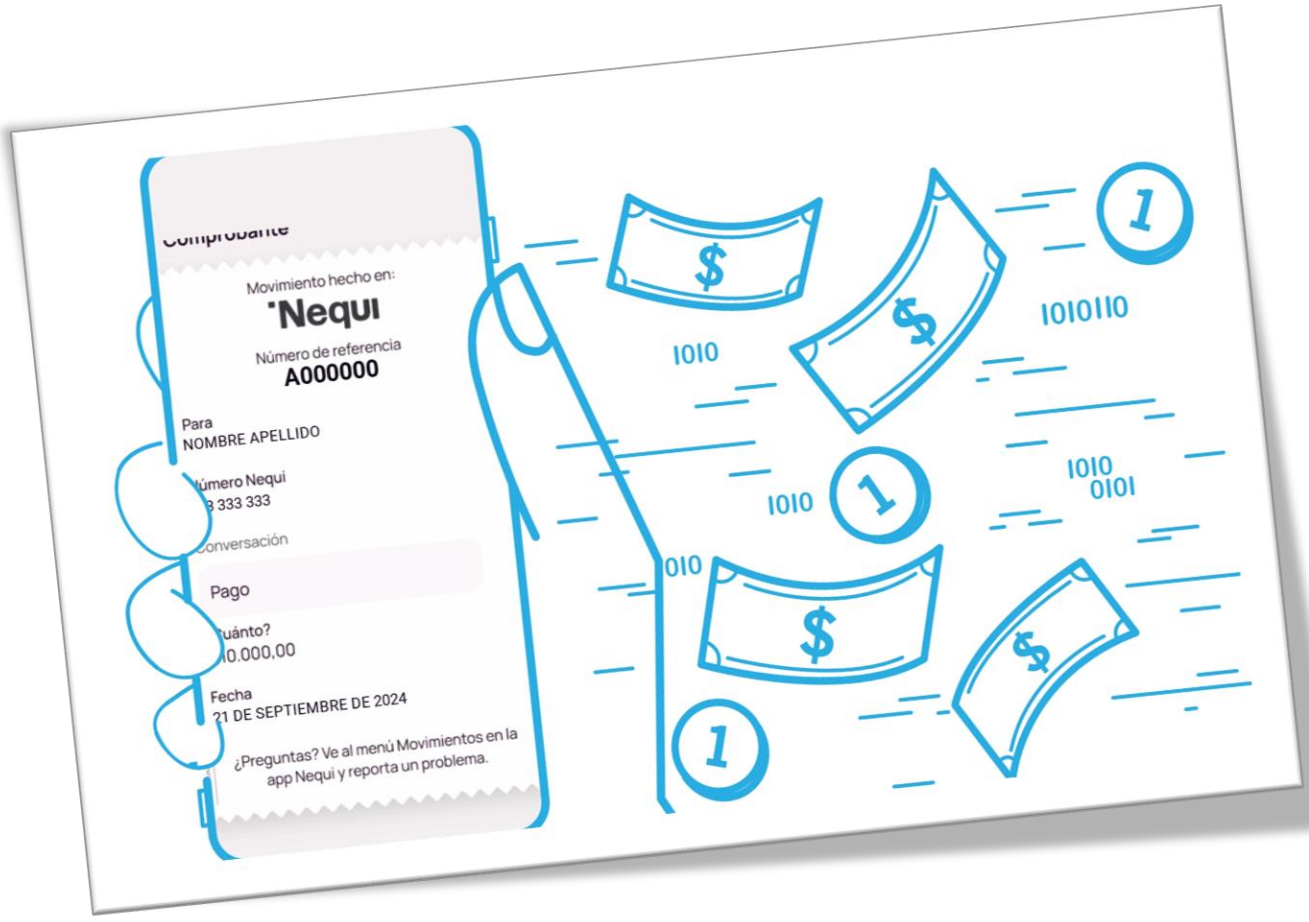
Una estafa de smishing puede ser fácil de ejecutar, difícil de rastrear y peligrosa en sus efectos. Un ataque de smishing exitoso puede exponer potencialmente sus contraseñas, fotos, vídeos y otros datos sensibles a un estafador y también funcionar como un vector de infección para una caída de malware en su teléfono inteligente.

SMISHING

ENVÍO DE RECIBOS BANCARIOS FALSOS

Este tipo de fraude cibernético consiste en la creación de recibos falsos en nombre de grandes empresas. Al realizar el pago, la víctima deposita el dinero en la cuenta de los estafadores.

Algunas versiones de este tipo de fraude pueden incluso implicar la creación de páginas falsas que simulan el entorno de la empresa, donde se redirige a las víctimas a descargar el documento falso sin levantar sospechas sobre la estafa.



SUPLANTACIÓN DE IDENTIDAD

Consejos para evitar la **Suplantación de identidad**

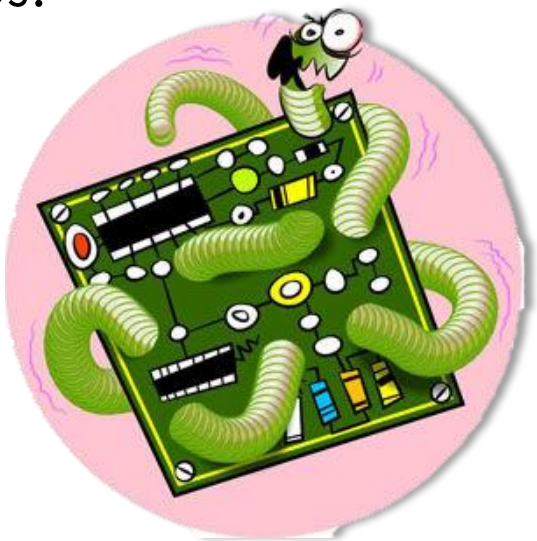
1. Denuncie la perdida de documentos a las autoridades en el menor tiempo posible.

2. Revise las políticas de privacidad de las plataformas digitales que utiliza.

3. Configure contraseñas seguras y active la verificación en dos pasos.

SABOTAJE INFORMÁTICO

Se trata de aquellos delitos cuyo propósito es alterar, modificar, borrar o suprimir información, programas o archivos de los equipos, a fin de impedir su funcionamiento normal. Se aplican para ello herramientas como los gusanos, las bombas lógicas y malwares.



El sabotaje informático puede incluir delitos tan graves como el ciberterrorismo, que tiene como propósito desestabilizar un país y generar un estado generalizado de conmoción nacional con fines inconfesables.

CIBER DELITOS

CIBERBULLYING

Acoso virtual, es un acto agresivo e intencionado, llevado a cabo de manera repetida a través del contacto electrónico por parte de un grupo o de un individuo contra una víctima que no puede defenderse fácilmente.

Se trata de un acto reiterativo de acosar, agredir y dañar a otra persona a través de medios telemáticos: internet, telefonía móvil, etc.

RANSOMWARE

El ransomware es un tipo de malware que mantiene como rehenes los datos o el dispositivo de la víctima, amenazando con mantenerlos bloqueados, o algo peor, a menos que la víctima pague un rescate al atacante.

INTERNET

¡Alerta!

Correo no deseado

La mayoría de estos correos ofrecen dinero de cuentas extranjeras u oportunidades de negocio. Pero su principal objetivo es robar información para suplantar tu identidad.

!Nunca envíes documentos o información personal a este tipo de correos para evitar afectar tu identidad¡

CONSEJOS PARA NAVEGAR SEGURO EN INTERNET

1. Utilice únicamente dispositivos de confianza para operaciones bancarias.
2. Verifique que las paginas tengan el símbolo del candado verde para la navegación segura.
3. No responda correos desconocidos que soliciten datos personales.
4. Cambien sus contraseñas periódicamente.
5. Tenga cuidado con los archivos que descarga.

La mejor protección, siempre será el sentido común.

Ciber seguridad

¡Cuidado!

Con los archivos adjuntos.

Los cibercriminales pueden ocultar malware en los archivos que recibe por correo electrónico. Tenga en cuenta estas recomendaciones para su seguridad digital:

1. Nunca descargue adjuntos de correos desconocidos.

2. Instale un programa antivirus en los dispositivos que utilice.

3. No ejecute archivos adjuntos con extensiones (.exe), suelen traer malware.

CONSEJOS PARA MEJORAR LA SEGURIDAD DE SUS CONTRASEÑAS

1. No utilice las mismas contraseñas en diferentes plataformas.
2. Habilite la autenticación en dos pasos en todas las cuentas.
3. Utilice un gestos de contraseñas para almacenarlas de manera segura.
4. Evite contraseñas de menos de ocho caracteres.
5. Convierta las vocales en números para aumentar la seguridad de las contraseñas.

Ciber seguridad

Su información es valiosa

¿Cómo protegerla?

1. Instale un antivirus en sus dispositivos para detectarlos a tiempo y evitar su ejecución.
2. Mantenga actualizado sus dispositivos y no descargue programas o aplicaciones de paginas desconocidas .
3. Realice una copia de seguridad de su información periódicamente.
4. En lo posible no utilice redes wifi publicas.

¿Que hacer si recibo amenazas por redes sociales?

1. Si sufre de amenazas, injurias, calumnias, extorsiones o ciberbullying, **!denuncie¡**

2. Mantenga la calma y no le siga el juego al ciberdelincuente que quiere intimidarle.

3. Guarde y conserve las conversaciones donde se evidencian las amenazas.

4. Reporte la cuenta en la red social y adjunte todas las evidencias recolectadas.

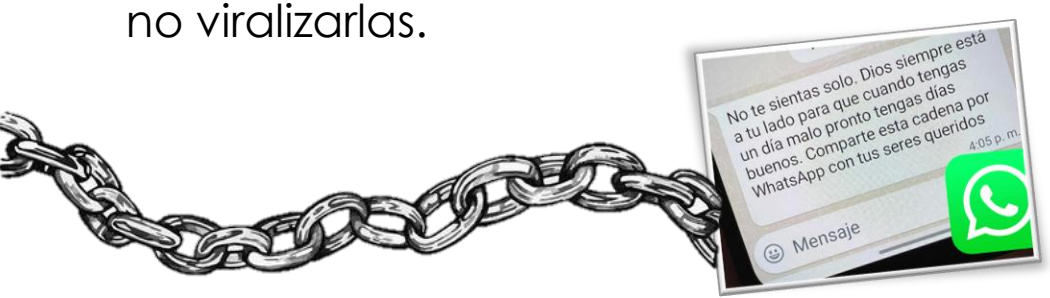
Ciber seguridad

Su información es valiosa

¿Cómo protegerla?

Las cadenas de mensajes en WhatsApp pueden ser un peligro para sus datos y la seguridad de sus dispositivo. Para evitar ser victima de estafas:

1. Tenga cuidado con promociones o promesas de regalos que reciba en cadenas.
2. Revise la URL antes de abrirla.
3. No descargue aplicaciones o ingrese datos sensibles si desconoce la procedencia.
4. Evite reenviar estas cadenas con engaños para no viralizarlas.



Consejos para proteger tu cuenta WhatsApp

1. Active la verificación en dos pasos en su cuenta.
2. Proteja su dispositivo con una de las opciones para la pantalla.
3. No comparta el código de verificación de su cuenta con nadie.
4. Active las notificaciones de seguridad para mantener su cuenta monitoreada.
5. Configure la copia de seguridad automática de los chats con su cuenta de correo

Ciber seguridad

Utilizando Facebook

De manera segura

1. ***Nunca divulgue información financiera por chats o publicaciones.***
2. ***No agregue ni acepte solicitudes de amista de personas que no conoce.***
3. ***Configure factores de recuperación en su cuenta como teléfono y correo.***
4. ***Verifique que solo sus amigos puedan acceder a sus fotografías y publicaciones.***
5. ***Configuración las alertas sobre inicios de sesión en dispositivos desconocidos.***

Principales peligros en INSTAGRAM

Sobreexposición

Compartir demasiada información privada como la ubicación en fotografías puede poner en riesgo la integridad física de los usuarios

Perfiles falsos

En los entornos digitales es difícil saber quien esta detrás de una fotografía realmente y estas cuentas pueden ser utilizadas para estafas.

Ciberacoso

Los depredadores sexuales están atentos a cualquier victima, para chantajear o amenazar por este media a cambio de dinero.

Tips de seguridad para su cuenta INSTAGRAM

Ciber seguridad

Perfil Privado

Esta medida permite tener un control total sobre quien puede ver su información

Opción de "mejores amigos"

Si tiene perfil publico, esta opción le permite elegir quienes pueden ver sus historias.

Actividad de inicio de sesión

Verifique periódicamente los dispositivos desde donde ha iniciado sesión para evitar accesos no autorizados a su perfil.

Verificación en dos pasos

Evite que tercero tengan acceso a su cuenta, en caso de que cibercriminales obtengan su contraseña.

INVITACIÓN

SESIÓN 7: PREVENCIÓN DEL SECUESTRO

25 SEPT 2025

BIBLIOGRAFÍA

- Ley 599 de 2000 Código Penal de Colombia – (Artículo 246 y siguientes).
- Ley 1273 de 2009 – marco para los delitos informáticos.
- Cámara Colombiana de Informática y Telecomunicaciones (CCIT)
- Policía Nacional – División de delitos informáticos / CAI Virtual.
- Fiscalía General de la Nación


POSITIVA
COMPAÑÍA DE SEGUROS
suma 5.0
educa
comunica
EVALUÉMONOS
Fórmulas para la vida
Valores + Emociones + Competencias
Respeto + Gratitud + Ética y sostenibilidad

PREGUNTAS

POSITIVA COMPAÑÍA DE SEGUROS | suma 5.0 | educa | comunica

Recuerda que POSITIVA tiene para ti:

Posipedia

https://posipedia.com.co/

- Cursos virtuales
- Artículos
- Audios
- Juegos digitales
- OVAS
- Guías
- Mailings
- Videos

POSITIVA COMPAÑÍA DE SEGUROS | suma 5.0 | educa | comunica

¿Quieres profundizar tus conocimientos y potenciar tus competencias en SST?

¡Capacítate y fortalece
la seguridad de tu empresa!

CURSOS

VIRTUALES SG-SST DE 50 Y 20 HORAS

Escanea e inscríbete

Para trabajadores de todas las empresas, áreas y sectores.

¡TE ESPERAMOS!

Positiva Prevención

Hacienda

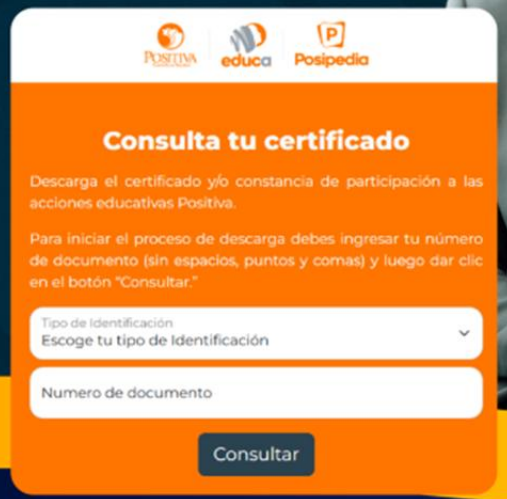
POSITIVA COMPAÑÍA DE SEGUROS | suma 5.0 | educa | comunica | Posipedia

Conoce cómo

descargar los certificados de las acciones educativas

01

02



03

Paso 1:
Escanea el código QR

Paso 2:
Selecciona el **tipo de documento** y escribe el **número**, una vez diligenciados da clic en consultar.

Paso 3:
Encontrarás tu historial académico y podrás generar la descarga de tu certificado en el icono