



SEGURIDAD DE LA INFORMACIÓN y CIBERSEGURIDAD

Clientes

Contenido

> 1 Qué es Seguridad de la Información y Ciberseguridad?

2 Riesgos asociados con los Clientes – Ingeniería Social

- Ciclo de Ataque Ingeniería Social
- Tipos de Ataques

3 ¿Cómo protegerte a nivel personal y laboral?

- Recomendaciones relacionadas con HDI SEGUROS
- Recomendaciones Generales
- Recomendaciones para uso de WIFI
- Recomendación para la creación de Contraseñas

4 ¿Cómo reportar incidentes o eventos relacionados con Seguridad de la Información?

1 Qué es Seguridad de la Información y Ciberseguridad?

¿Qué es Seguridad de la Información (SGSI) y Ciberseguridad?

Seguridad de la Información - SGSI

Seguridad de la Información es una buena práctica y la definición de controles establecidos por las organizaciones como políticas, estrategias, metodologías, recursos, soluciones informáticas, prácticas y competencias.

El SGSI es el **Sistema de Gestión de Seguridad de la Información** que permite el aseguramiento, de la **confidencialidad**, **integridad** y **disponibilidad** de la información, así como de los sistemas que la procesan.

Ciberseguridad

Framework for Improving Critical Infrastructure Cybersecurity NIST.

Proceso para proteger la información **previniendo**, **detectando** y **respondiendo** frente a un **ataque**.

Circular Externa 007 de 2018 Colombia

Es el desarrollo de capacidades empresariales para **defender** y **anticipar** las **amenazas cibernéticas** con el fin de proteger y asegurar los datos, sistemas y aplicaciones en el ciberespacio que son esenciales para la operación de la entidad.

2 Riesgos asociados con los Clientes – Ingeniería Social

Riesgos asociados con los Clientes – Ingeniería Social

Todas las personas estamos expuestas a diversos riesgos relacionados con su información personal, financiera, familiar, entre otras y personas ajenas utilizando diferentes métodos, aprovechan el desconocimiento en estos temas.



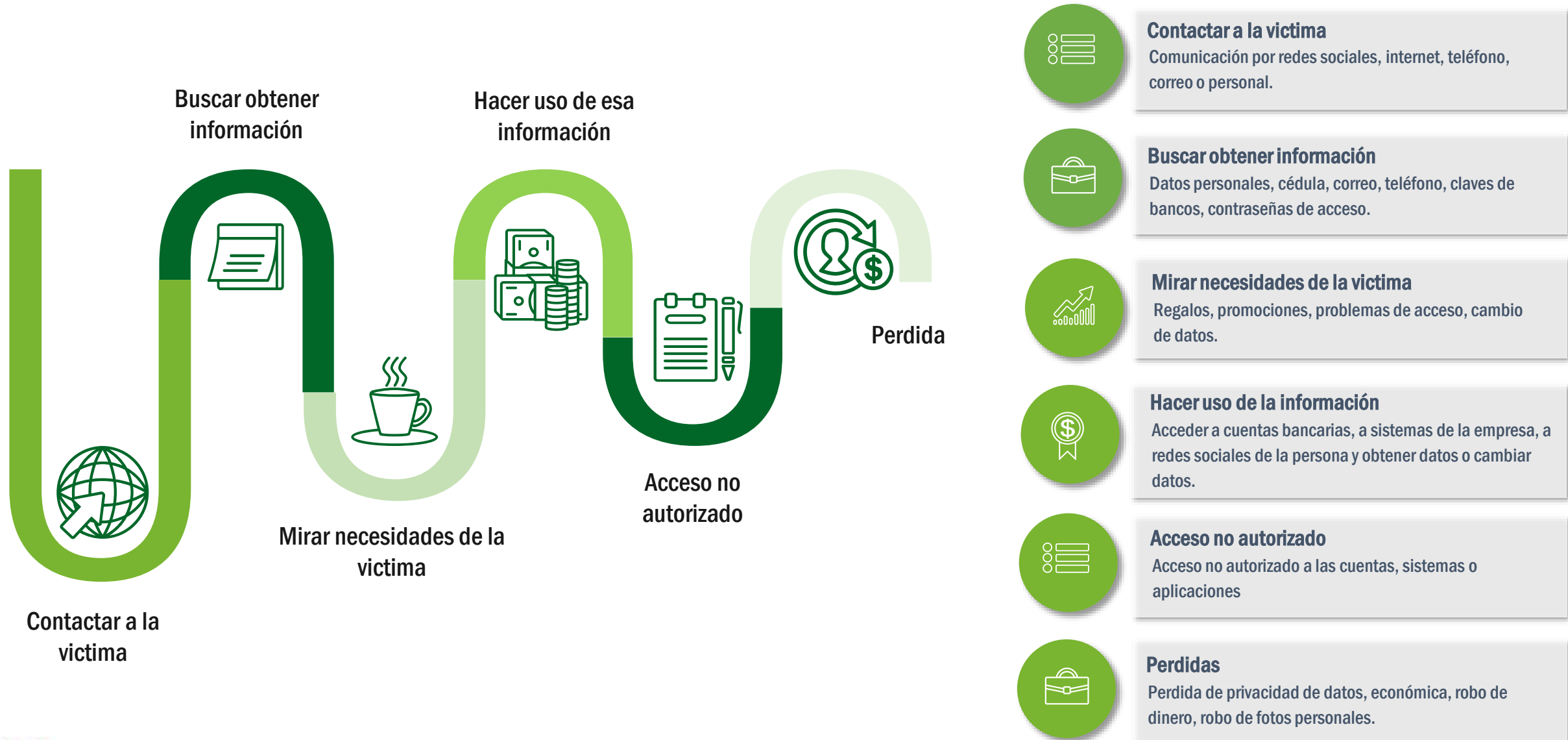
POR INGENIERÍA SOCIAL: Se utiliza la psicología humana para conseguir información:

“Buenos días le ofrecemos la renovación para el seguro de su automóvil y un descuento del 10%, si cancela hoy el valor de la prima.

Es el acto de engañar a la gente para que haga algo que no desea o para que proporcione información.

Si recibe una llamada, correo electrónico o un mensaje de WhatsApp de nuestra parte que le genere alguna inquietud, no dude en contactarnos o preguntarle a su Intermediario de Seguros.

Riesgos asociados con los Clientes – Ingeniería Social - Ciclo de ataque



Riesgos asociados con los Clientes – Ingeniería Social – Tipos de Ataques

1

Pretexting

Base de cualquier ataque de Ingeniería social

2

Dumpster diving

Acto de “husmear” en la basura

3

Shoulder surfing

Consiste en “espiar” físicamente a la persona

4

Baiting

Emplea un cebo con software malicioso



Redes Sociales

Engaño mediante cupones de descuento.

5

Phishing

Busca “pescar” víctimas

6

Vishing

Llamadas telefónicas

7

Smishing

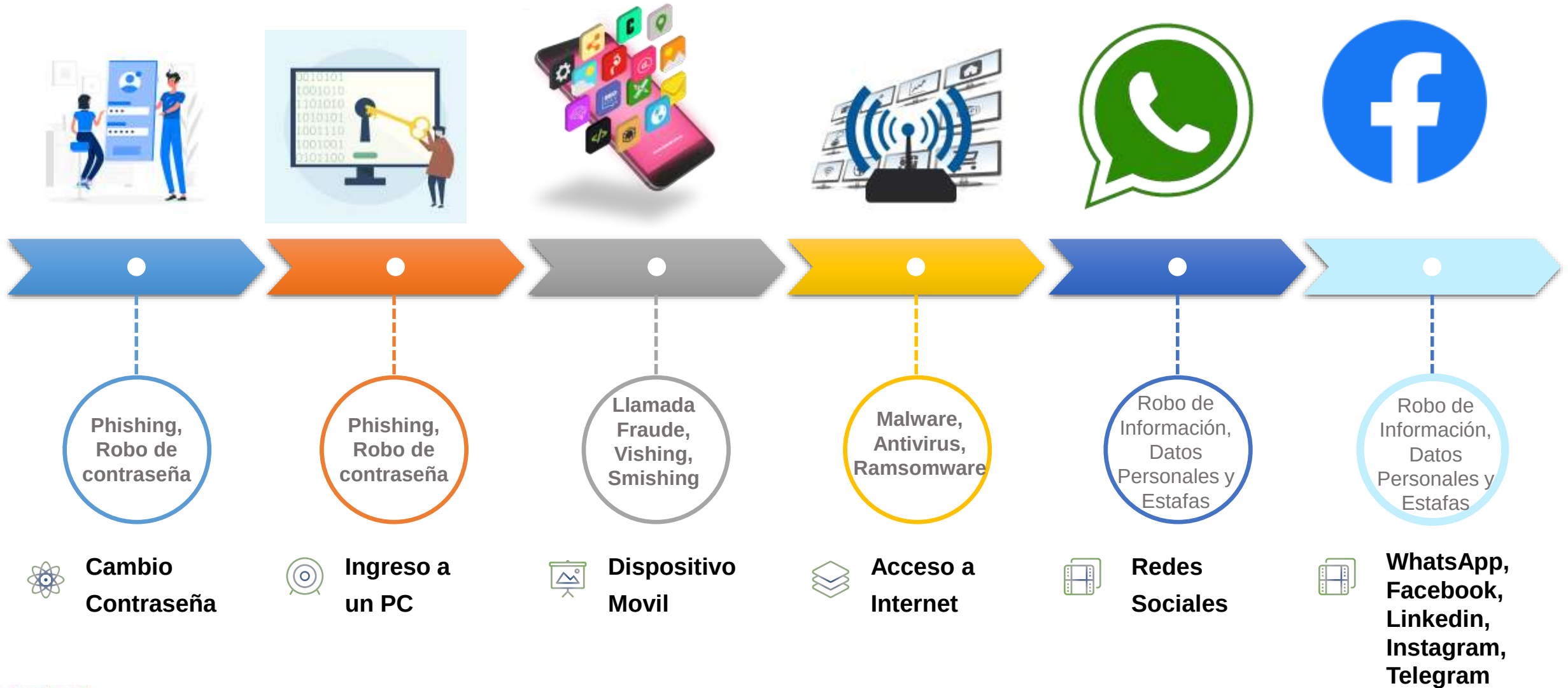
Variante del “phishing” pero que se difunde a través de SMS.

8

Sextorsión

Chantaje donde amenazarán a la víctima

Riesgos asociados con los Clientes – Ingeniería Social – Tipos de Ataques



Riesgos asociados con los Clientes – Ingeniería Social – Tipos de Ataques

POR REDES SOCIALES

SEXTING: Envío de imágenes personales por redes.



GROOMING: Contacto de un adulto con un niño con interés sexual.



CYBERBULLYING: El uso de los medios telemáticos para ejercer el acoso psicológico entre iguales.



Riesgos asociados con los Clientes – Ingeniería Social – Tipos de Ataques, Ejemplos de Phishing

Mira 😍😍

La oferta es solo durante el día de hoy así que si queréis aprovechar y echar un vistazo ya sabéis.

⇒ <http://zara.com-free-gratuito.com>

¡Espero que os resulte muy útil!

22:09

Hola,

Por favor mira el documento que subí para ti usando Google docs, **PULSA AQUI** y regístrate con tu correo electrónico para ver el documento, es muy importante

Saludos

Último Aviso: 11/04/2016

Estimado Contribuyente:

El Servicio de Administración Tributaria se ha percatado que en diversos despachos alrededor del País, Usted ha propuesto esquemas para **evadir el pago de impuestos** y hemos detectado **anomalías en su situación fiscal**. Para evitar una sanción en su contra, Le recomendamos regularizar esta situación de inmediato. A continuación le adjuntamos un documento detallado de su situación fiscal actual.

[Descargar Documento.](#)

© Derechos Reservados SAT - Servicio de Administración Tributaria

Microsoft

Error con su buzón- June 19, 2018

Habilite su archivo

Habilite el archivo de su buzón para evitar perder su correo electrónico. Después de que el archivo de un usuario esté habilitado, está disponible hasta 100 GB de almacenamiento adicional.

ID: asnet@asnet.es
Time: 20:44

Con un solo clic, estará listo y su almacenamiento adicional se configurará automáticamente

Habilitar hoy

<https://screensmart.com.au/use.php?email=asnet@asnet.es>

Gracias,

Riesgos asociados con los Clientes – Ingeniería Social – Tipos de Ataques, Malware

Del inglés malicious software, también llamado badware, código maligno, software malicioso o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario.

Tipos de Malware

Virus

“Programa malicioso que Infecta a un equipo para dañarlo u obtener control”

Trojanos

“Programa que se camufla hasta que el atacante desee que se ejecute para tomar control”

Gusanos

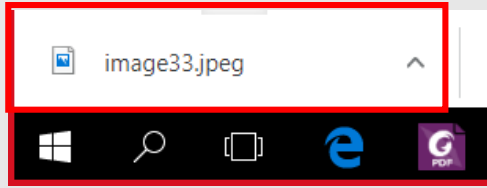
“Programa que se puede replicar a otro equipo por sí mismo por la red”

Ransomware

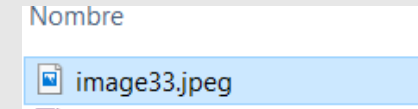
“Programa que impide a los usuarios acceder a su equipo o a sus archivos personales y que exige un rescate para poder acceder a ellos”

Riesgos asociados con los Clientes – Ingeniería Social – Tipos de Ataques, Ejemplos de Malware

Se abre el archivo o la USB
Se descarga el archivo



Se da click en el link o archivó
Se abre el archivo con el virus

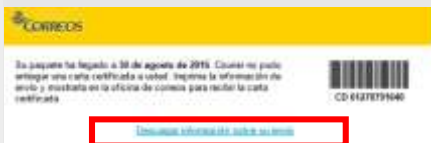


No se detecta

No se reviso el remitente o se evaluó si es un fraude.

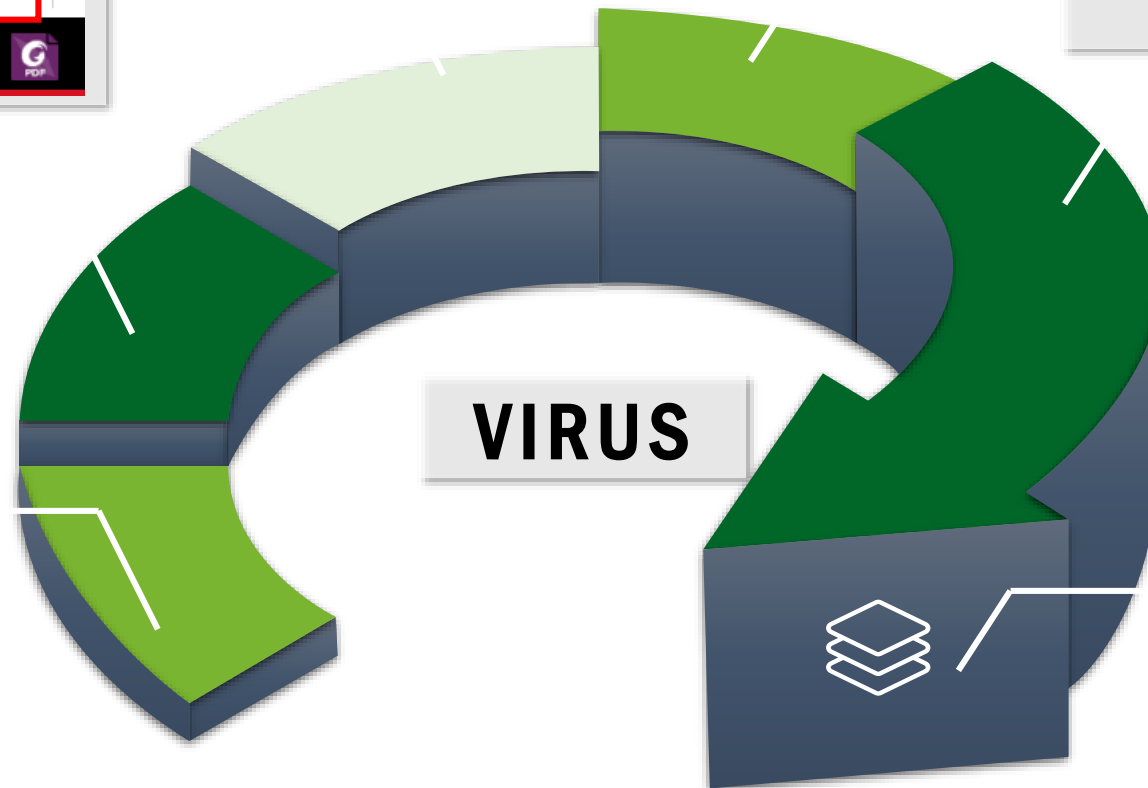


Se recibe un mensaje o se conecta algo al PC
Correo electrónico con link para realizar descarga.



El virus se ejecuta

Se inicia el proceso de propagación del virus en la maquina



Perdida

Perdida de información., piden rescate por ella.



Riesgos asociados con los Clientes – Tipos de Ataques, afectación de disponibilidad de servicios

Tras ataque cibernético, DANE recupera su página web

La entidad mencionó en un trino que siguen “adelantando procesos de actualización en algunas secciones. Agradecemos su comprensión”.

Tras ciberataque, Universidad Javeriana deshabilitó algunos servicios

Tras el incidente, la institución dijo que no hay evidencia de fuga o pérdida de información. FOTO: Getty Images

Los sistemas de la actividad central de la institución se mantienen protegidos.



Riesgos asociados con los Clientes – Tipos de Ataques, afectación de disponibilidad de servicios



Origen

El ataque puede presentarse a cualquier persona.



Propagación

Varios virus informáticos se pueden comparar con el covid 19, si no se detiene a tiempo o se controla se propaga por todas partes.



Por donde puede ingresar

Equipos no actualizados, personas que utilicen el equipo para navegar en sitios no adecuados, o bajar programas piratas



Que ocasiona

El secuestro de datos, modificando la información para que no pueda ser utilizada por la persona si no se paga un rescate.



Se puede detener

Si no se siguen buenas practicas, y se toman medidas tarde, la forma de contenerlo es no permitir que las personas trabajen hasta que se solucione.



Pérdidas

Las perdidas son económicas por que los procesos se paran, a su vez puede que la información nunca se recupere.



3 ¿Cómo protegerse a nivel personal y laboral?

¿Cómo protegerse a nivel personal y laboral?

Recomendaciones relacionadas con HDI SEGUROS

- ✓ Para ingresar a nuestra página web digite en la barra de direcciones del navegador www.hdi.com.co
- ✓ Realizar la compra de sus seguros en los puntos autorizados de HDI SEGUROS, los cuales puede consultar en nuestra página web www.hdi.com.co
- ✓ Identificar al personal que lo atiende en las Sucursales o Centros de Negocios HDI con el carnet de la entidad o si adquieres el seguro a través de un Intermediario puede validar que se encuentre autorizado por la Compañía, en nuestra página web.
- ✓ **Al realizar pagos hacia la Compañía valide previamente que esté dentro de los medios de recaudo autorizados en nuestra página web.**



Recomendaciones Generales

Hacer uso de herramientas online para efectuar consultas, transacciones u operaciones es seguro, siempre y cuando tenga en cuenta ciertas precauciones para no caer en manos de personas malintencionadas o Hackers. Tenga en cuenta las siguientes recomendaciones en general:

- ✓ Para reconocer que una página en Internet es segura, revise en la parte superior de la pantalla, que allí aparezca un candado que indica que en ese momento su conexión es segura. Esto demuestra que la información que viaja desde su computador al servidor consultado está siendo cifrada.
- ✓ Otra característica que indica que la conexión es segura, es que en el campo de la dirección de la página en Internet inicia con las letras HTTPS.
- ✓ Escriba directamente en el buscador de la Web la dirección de la página que desea consultar, no realice conexión a través de enlaces (link) que puedan llegar a través de algún correo electrónico.

¿Cómo protegerse a nivel personal y laboral?

Recomendaciones Generales

- ✓ No realice transacciones personales o financieras en sitios que no sean de su absoluta confianza, pues en ellos existe el riesgo que puedan grabar sus datos e información financiera, los cuales posteriormente pueden usar en su nombre y generar un fraude.
- ✓ Recuerde actualizar el navegador de Internet para obtener mayores ventajas en cuanto a seguridad y servicios de navegación.
- ✓ Evite abrir archivos adjuntos que se envíen en cadenas, estos pueden ser virus. Por el contrario, trate siempre de navegar de forma segura en computadoras o dispositivos móviles con antivirus.
- ✓ Utilice protector de pantalla de su computadora o dispositivo móvil con clave y que se active algunos segundos después de haber dejado de usarlo.
- ✓ Realice un análisis y limpieza de sus dispositivos apoyándose en su antivirus.
- ✓ Recuerde que sus claves y datos personales son confidenciales. No los comparta con cualquier persona a través de ningún medio como internet, correos electrónicos, teléfono, encuestas, entre otros. Tenga en cuenta que son personales e intransferibles.
- ✓ Cambie sus claves periódicamente, es una buena práctica y evita que éstas sean vulneradas.
- ✓ Absténgase de responder correos que soliciten su información confidencial, así estos parezcan provenir de una entidad con la cual tenga relación alguna.
- ✓ No descargue archivos provenientes de páginas web que no conozca.
- ✓ Ingrese a los diferentes canales que requiera a través de sitios de su absoluta confianza.
- ✓ Cuando finalice su consulta, transacción u operación, cierre el navegador (Programa que le permite utilizar los servicios de Internet) y verifique que su sesión ha sido cerrada.
- ✓ No preste sus credenciales de acceso en aplicaciones o APP como el Usuario y Contraseña.



¿Cómo protegerse a nivel personal y laboral?

Recomendaciones para el Uso de WIFI

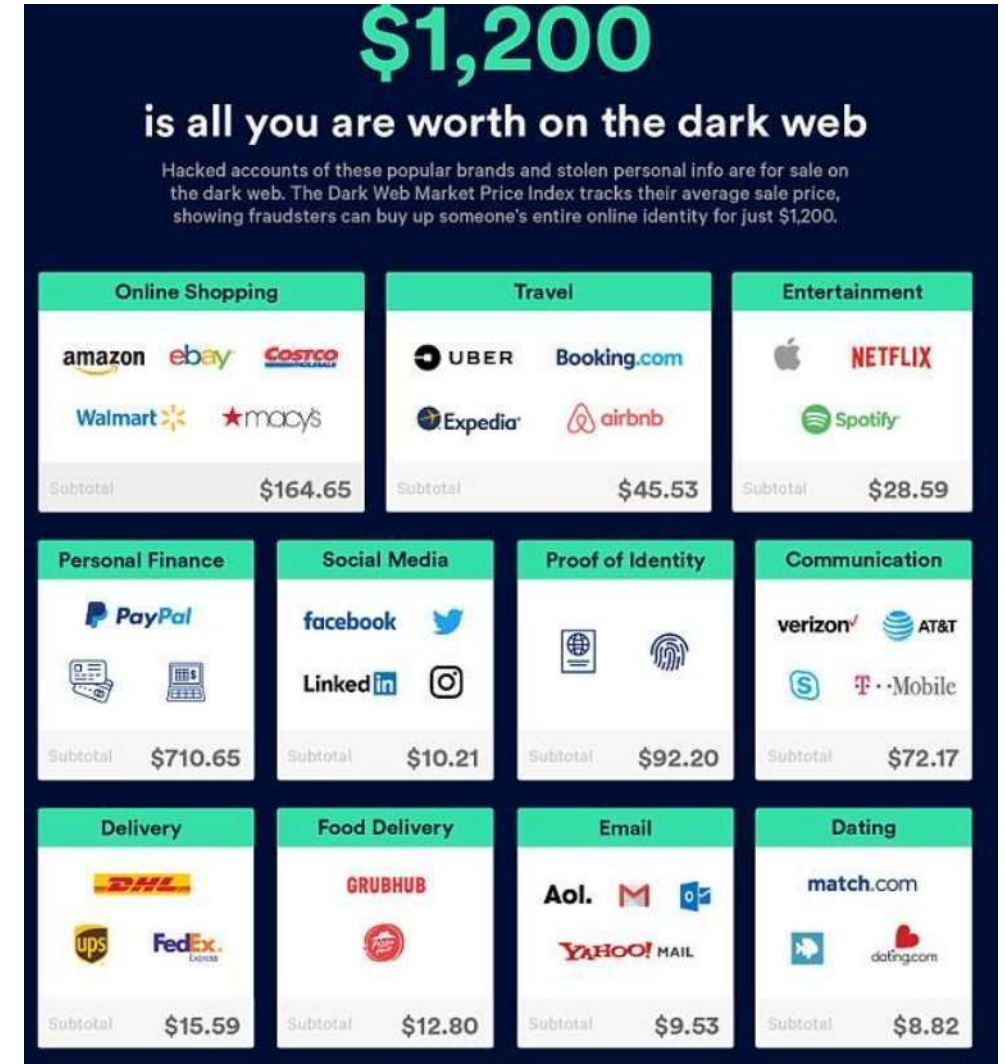
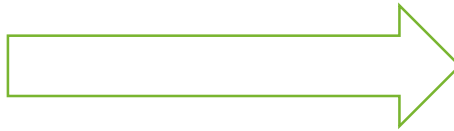
1. Verifique el nombre de la red wifi con el propietario antes de conectarse.
2. Trate todas las conexiones wifi públicas como si fueran maliciosas
3. Siempre utilice una solución antimalware para prevenir ataques cibernéticos mientras está conectado



¿Cómo protegerse a nivel personal y laboral?

Recomendaciones Generales

No utilice su cuenta de correo en sitios inseguros, ya que pueden robar sus credenciales de acceso y venderlas en sitios fraudulentos.



¿Cómo protegerse a nivel personal y laboral?

Recomendación para la creación de Contraseñas

1. Letras mayúsculas

A, B, C, D, E

2. Letras minúsculas

a, b, c, d, e

3. Números

0, 1, 2, 3, 4

4. Caracteres especiales

‘/ % & \$ # @ : > * ☹ < 3 - +

Al menos una cadena compuesta por 10

1 No se deben prestar a otros usuarios

2 No se deben guardar en papeles o stickers de colores

3 No se deben guardar debajo del teclado

4 No se deben guardar en el equipo en un Excel, menos si se llama claves

No utilizar palabras conocidas

- ✓ Fechas de nacimiento
- ✓ Nombres y apellidos
- ✓ Datos familiares
- ✓ Datos laborales
- ✓ Combinaciones comunes como:
 - Seguros2021 Julio2020
 - Bogota2022 Abcd1234

4 ¿Cómo reportar incidentes o eventos relacionados con Seguridad de la Información?

¿Cómo reportar incidentes o eventos relacionados con Seguridad de la Información?

En HDI SEGUROS pensamos en su seguridad. Por eso, si detecta casos o conductas sospechosas, al ingresar a nuestras instalaciones o a nuestras aplicaciones web no dude en comunicarse con nosotros al siguiente correo: Seguridad@hdi.com.co





GRACIAS

Teiddy Calderón | Bogotá | 01.12.2021

