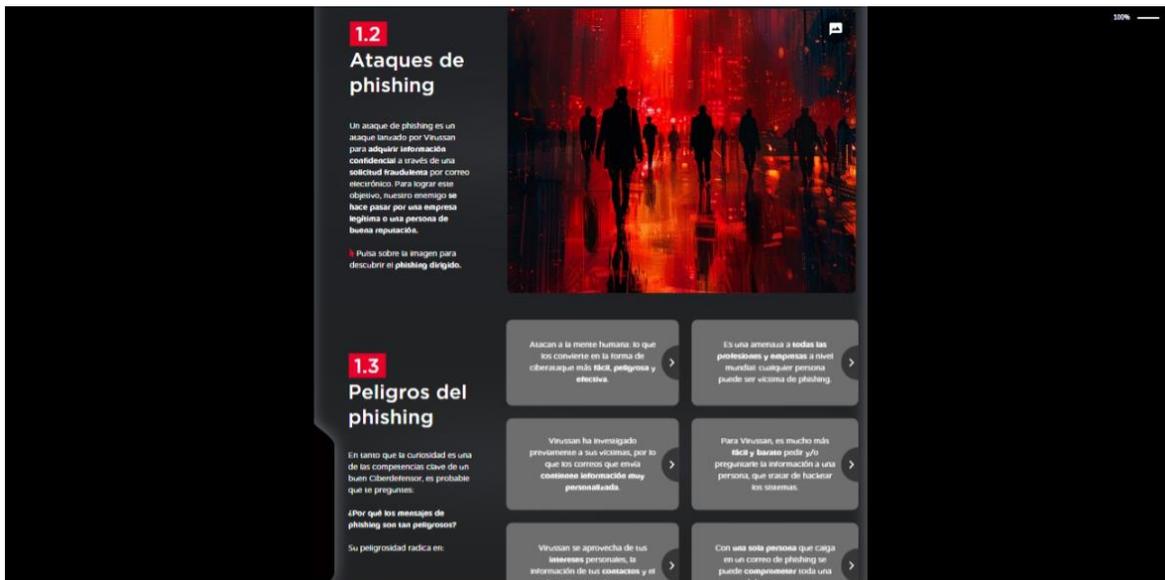


Cybersecurity training

Contents:

- Chapter 1: Information Security Attacks
- Chapter 2: Security Controls
- Chapter 3: Information Security Recommendations
- Chapter 4: Information Security measures for remote and office work



1.2 Ataques de phishing

Un ataque de phishing es un ataque lanzado por Viruscan para robar información confidencial a través de una solicitud fraudulenta por correo electrónico. Para lograr este objetivo, nuestro enemigo se hace pasar por una empresa legítima o una persona de buena reputación.

• Pasa sobre la imagen para descubrir el phishing dirigido.

1.3 Peligros del phishing

En tanto que la curiosidad es una de las competencias clave de un buen Ciberdefensor, es probable que te preguntes:

¿Por qué los mensajes de phishing son tan peligrosos?

Su peligrosidad radica en:

- Ascan a la mente humana, lo que los convierte en la forma de ciberataque más fácil, peligrosa y efectiva.
- Es una amenaza a todas las profesiones y empresas a nivel mundial cualquier persona puede ser víctima de phishing.
- Viruscan ha investigado previamente a sus víctimas, por lo que los correos que envía contienen información muy personalizada.
- Para Viruscan, es mucho más fácil y barato poder ya preguntarte la información a una persona, que tratar de hackear los sistemas.
- Viruscan se aprovecha de tus intereses personales, la información de tus contactos y el rol que desempeñas en tu empresa.
- Con esa sola persona que carga en un correo de phishing se puede comprometer toda una red de usuarios.



1.1 ¿En qué consiste la Política de Seguridad de la Información?

Esa política contiene las tres responsabilidades clave del buen Ciberdefensor:

- En primer lugar, vigilar la protección de la información de Banorte y de sus clientes en términos de confidencialidad, integridad y disponibilidad.
- En segundo lugar, asegurar la resiliencia de los servicios, procesos tecnológicos, operativos y de negocio, haciendo uso eficiente de los recursos mediante la administración de riesgo a un nivel aceptable para el negocio.
- Por último, impulsar una cultura de seguridad de la información y asegurar el cumplimiento con el marco normativo, regulatorio y legal aplicable.

1.2 Los Controles Administrativos te recuerdan

¡Qué sorpresa! Parece que hemos recibido una notificación por parte de Controles Administrativos:

• Pasa sobre la imagen para descubrirla.

Cada año, todos debemos leer y firmar la política de Seguridad de la Información a través de la intranet corporativa. Pero eso no es todo! También debemos actuar de acuerdo con sus principios, aplicando en todo momento uno de los mantras de Missacra: **¡Si es sospechoso, es peligroso!**

• [Da clic aquí para consultar la política](#)

0.3 Certificaciones Banorte

3.1 ISO 27001 - SASI

SASI son las siglas de Sistema de Administración de Seguridad de la Información, una poderosa herramienta de combate contra los ataques. Es el sistema mediante el cual se establecen reglas y se implementa, opera, monitorea, revisa, mantiene y mejora la Seguridad de la Información de acuerdo de acuerdo con el fin de alcanzar los objetivos de negocio.

Se encuentra alineado a la norma internacional ISO 27001, cuyo objetivo es preservar la confidencialidad, la integridad y la disponibilidad de la información para el logro de los objetivos de seguridad planeados en la institución.



3.2 PCI

Payment Card Industry Data Security Standard o PCI DSS es un estándar de seguridad que nos ayuda a minimizar el fraude con las tarjetas de crédito y débito.

¿Cuál es su cumplimiento?

Como banco, procesamos, almacenamos o transferimos información de los datos de las tarjetas de crédito y débito de nuestros clientes.

Por lo tanto, debemos cumplir este estándar y aplicar los principios básicos de Seguridad de la Información: confidencialidad, integridad y disponibilidad.



0.5 Seguridad en el uso del correo electrónico corporativo

5.1 Riesgos de usar mi correo corporativo fuera del trabajo

Como ya puedes imaginar, mantener seguro nuestro correo electrónico corporativo es de extrema importancia. Son varias las razones que podemos mencionar: protegemos nuestros datos personales y laborales, prevenimos fraudes y estafas, y protegemos nuestra identidad digital, entre otras muchas cosas.

Para combatir los riesgos que Viruscan puede plantearnos, síbre todo cuando usamos el correo electrónico fuera del trabajo, primero debes conocernos bien. Te los mostramos todos aquí.

01

Si usamos nuestra cuenta laboral en alguna plataforma de servicios y esta es atacada o vulnerada por los hackers, ellos podrían tratar de ingresar a nuestro correo laboral usando la información que obtuvieron.

5.2 Tips de seguridad

Ya estamos casi terminando la misión, futuro Ciberdefensor! Para mantener siempre seguro tu correo electrónico, aplica estos consejos en tu día a día:



Evita usar tu dirección de correo electrónico laboral para servicios personales o suscripciones.



Usa contraseñas fuertes y robustas y no las compartas, evita usar la misma contraseña de tu correo laboral para otros servicios.



Mantén atento a cualquier actividad sospechosa en tu correo. Reporta inmediatamente.



Evita usar tu correo laboral en redes Wi-Fi públicas, pues son el objetivo principal de Viruscan para robar.

1.2 Las tres claves

Ahora que conoces los peligros a los que te enfrentas, te mostraré sus puntos débiles a través de algunas recomendaciones clave para resguardar la información mientras trabajas desde casa.

Establece una conexión de red segura a través de tu equipo de cómputo corporativo y por medio de la VPN (red privada virtual).

Utiliza conexiones de internet personales (internet de casa o internet compartido) a través de un smartphone evitando redes públicas.

De ser posible, designa un espacio o cuarto de tu casa como lugar de trabajo, de preferencia que cuente con puerta, ya que eso evitará que la información que sea mencionada en las juntas de trabajo (videoconferencias y audiokonferencias) sea escuchada por terceros personas.

Clasifica tu reunión de acuerdo con el tipo de información (pública, interna, confidencial, privilegiada) que se va a mencionar por parte de los participantes.

Limita el número de participantes en los reuniones a solamente las personas estrictamente necesarias.

Reto

¡Ponte a prueba!

¿Eres capaz de identificar al enemigo? Compruébalo con el siguiente reto en el que tendrás que decidir si la situación que se te presenta es un peligro o no.

- Decide si las siguientes situaciones son un peligro o una práctica recomendable.



3.2 Seguridad por defecto

El término seguridad por defecto se refiere a un modo de actuar y hacer las cosas, consta de los siguientes principios:

La Seguridad de la Información en nuestros labores diarios debe estar desde el inicio, es decir, desde que llegamos y encendimos la computadora, no puede ser después.

La Seguridad de la Información no es una meta, sino un proceso que está presente de forma continua durante toda nuestra jornada laboral.

No debemos suponer que la seguridad se implementa sola o es responsabilidad de alguien más.

Siempre nos mantenemos actualizados en materia de Seguridad de la Información y estamos atentos a las nuevas formas de ataque a la información.

3.3 Incidentes de Seguridad de la Información

Avanza en la galería para conocer qué son y por qué se originan los incidentes de seguridad de la información.

Además, podrás descubrir cuáles son nuestras líneas de defensa para protegernos de ellos.

Nuestras líneas de defensa

- SOC (Security Operations Center)
- ERT (Equipo de Respuesta a Incidentes) genera plan de respuesta
- Ciber crisis: Implementa plan de respuesta