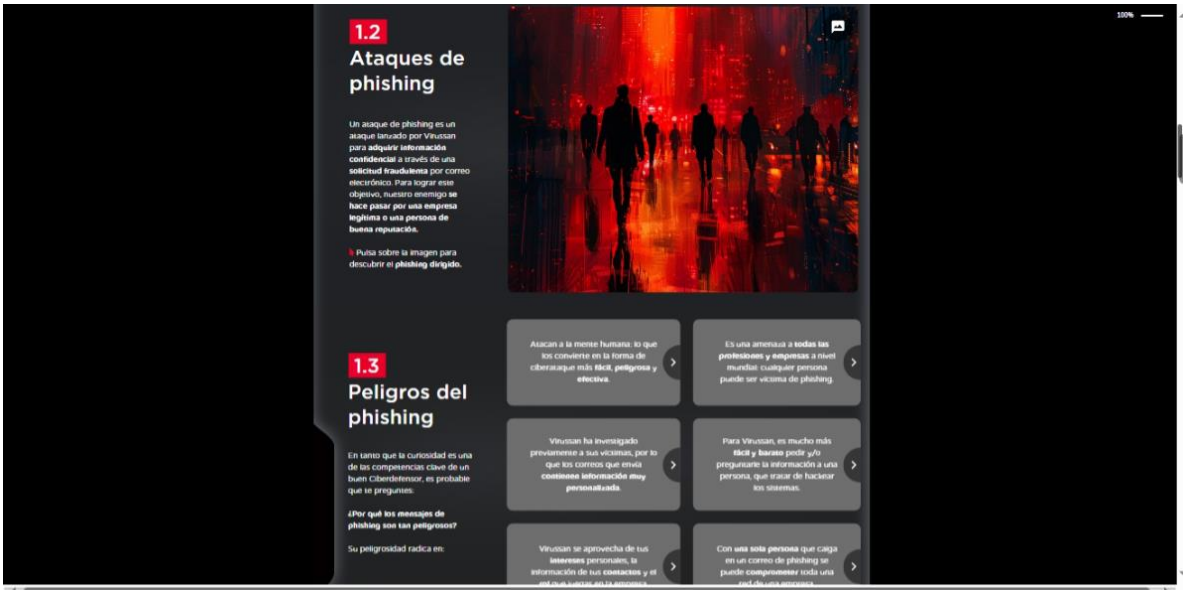
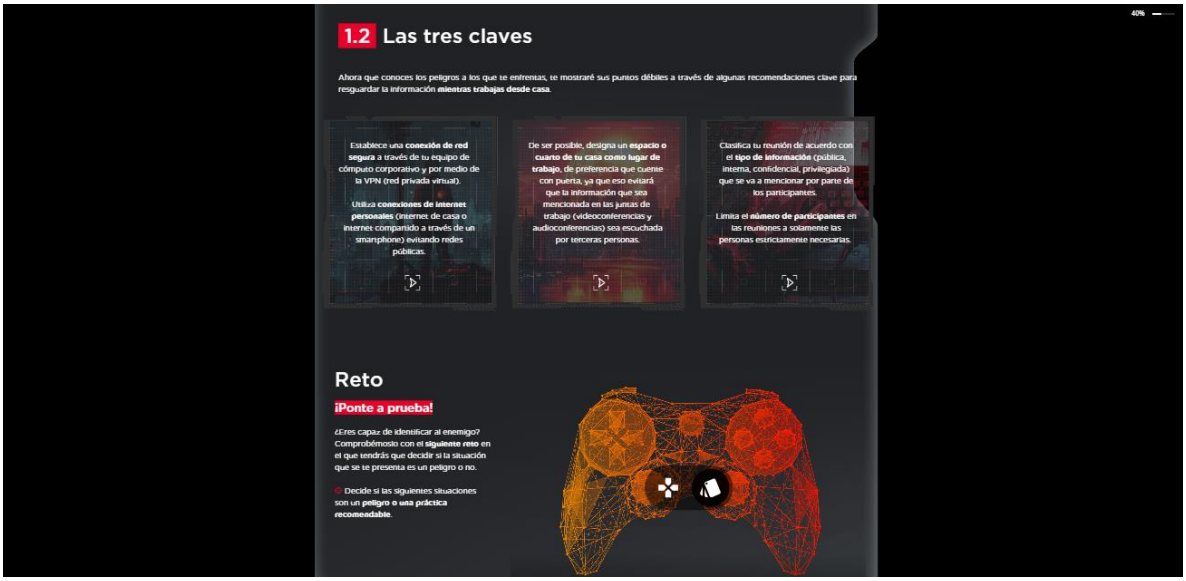
Cybersecurity training

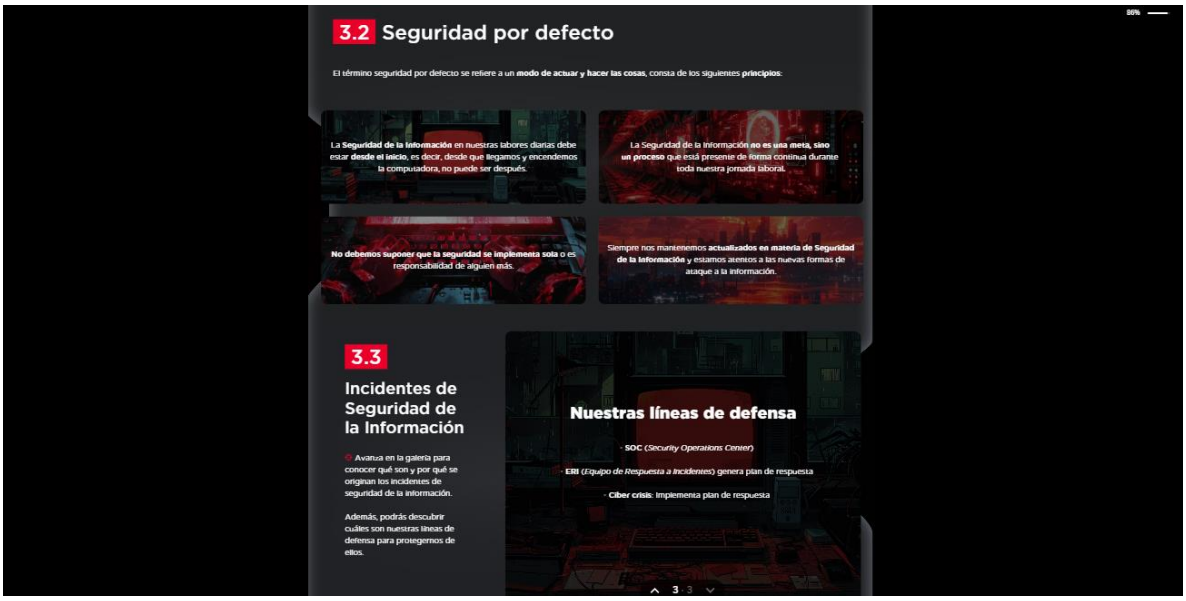
Contents:




03 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 dentro de Banorte 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.
¿Cuáles son los objetivos del SASI?
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.


05 Seguridad en el uso del correo electrónico corporativo
5.1 Riesgos de usar mi correo corporativo fuera del trabajo
Como te 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 Virussan puede plantearnos, sobre todo cuando usamos el correo electrónico fuera del trabajo, primero debes conocerlos bien. Te los muestro todos aquí:
01
Si usamos nuestra cuenta laboral en alguna plataforma de servicios y esa 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.
Mantente atento a cualquier actividad sospechosa en tu
Evita usar tu correo laboral en redes WiFi públicas, pues son el objetivo primordial de Virussan para robar


40%
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 audioconferencias) sea escuchada por terceras 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 las reuniones a solamente las personas estrictamente necesarias.
Reto
¡Ponte a prueba!
¿Eres capaz de identificar al enemigo? Comprobémoslo 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.


89%
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 nuestras labores diarias debe estar desde el inicio, es decir, desde que llegamos y encendemos 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)
- ERI (Equipo de Respuesta a Incidentes) genera plan de respuesta
- Ciber crisis: Implementa plan de respuesta
3 3