Capacitación Aeropuerto

Seguridad de la Información

REV.00 01.01.2021

Confidential Disclaimer

Esta capacitación y todo su material son para el uso exclusivo de la Empresa y puede contener información privilegiada o confidencial. Si has recibido por error este material, avísanos de inmediato, elimina enseguida este documento y abstente de hacer copias o de divulgar su contenido.

Objetivo de desempeño:

Mejorar el nivel de conocimiento de los empleados y colaboradores sobre Seguridad de la Información e indicar cuáles son los principales ataques a los que se encuentran expuestos, tanto dentro como fuera de la empresa.

Al completar este curso podrás:

- *Conocer la política de Seguridad de la Información.*
- *Identificar los conceptos claves de Seguridad de la Información.*
- *Detectar amenazas de seguridad e identificar cómo actuar ante un potencial incidente.*
- *Aplicar mejores prácticas para la protección y el resguardo de información sensible.*

¿Sabías qué para los atacantes, los empleados y colaboradores de las empresas son los principales blancos para un ataque exitoso?

Por eso es necesario estar siempre atentos y no ser víctimas de estos tipos de ataque…

Seguridad de la Información

Módulo I

Introducción a la Seguridad de la Información

¿Qué es la Seguridad de la Información?

La **Seguridad de la Información** es un conjunto de medidas preventivas para proteger la información de la compañía de las diversas amenazas a las que se enfrenta.

La Seguridad, más allá de ser un principio fundamental para todas las empresas, debe ser parte del día a día de todos los colaboradores de la compañía.

Por esto es importante que conozcamos las políticas de seguridad de la información, como también las normas y procedimientos que la soportan.

¿Cuáles son los principios de Seguridad de la Información?

Estos son los principios fundamentales de la Seguridad de la Información, en ellos debe apoyarse la evaluación de todo proyecto, sistema o proceso:

CONFIDENCIALIDAD

INTEGRIDAD

DISPONIBILIDAD

Principios de Seguridad de la Información

CONFIDENCIALIDAD

Reservar el acceso a la información solamente a personas, procesos, proveedores a los sistemas autorizados.

Ejemplo: preservar los datos de todos los clientes, los cuales son información sensible que solo deber ser utilizada en los procesos específicos que así lo requieran y por las personas que cuenten con la autorización correspondiente.

Principios de Seguridad de la Información

INTEGRIDAD

Proteger la información contra modificaciones o alteraciones indebidas, garantizando su autenticidad.

Ejemplo: garantizar que la información entregada por el cliente al hacer alguna transacción sea íntegra. Para ello, esta información debe almacenarse en la base de datos de la compañía, de tal manera que solo pueda ser editada en caso de contar con autorización.

Principios de Seguridad de la Información

DISPONIBILIDAD

Garantizar el acceso oportuno y confiable a la información cuando sea necesario.

Ejemplo: garantizar que el proceso de transacción esté disponible durante todo momento. Esto es crucial para evitar impactos operacionales que podría acarrear el no poder completar el procedimiento a tiempo.

Seguridad de la Información en Grupo LATAM

El Grupo LATAM es consciente de la importancia de proteger la información y está comprometido en cumplir esta tarea.

Para ello, cuenta con un área que se encarga de resguardar la seguridad de los datos de la compañía y de mantener su confidencialidad, disponibilidad e integridad.

La política de Seguridad de la Información del Grupo LATAM establece las directrices para la protección de la información de la compañía.

En ella se establecen los principios básicos para asegurar la confidencialidad, la integridad y la disponibilidad de la información a través del uso de mejores prácticas y tecnologías disponibles.

Seguridad de la Información en Grupo LATAM

Los repositorios autorizados para el almacenamiento dentro deLATAM son Google Drive y Fileshare .

¿Cómo está compuesta la política de seguridad de la información ?

Se compone de diversas normativas y procedimientos , que permiten indicar lo que se debe proteger , quien debe hacerlo, como y porqué.
Se accede a ella a través de:
Portal LATAM > Compliance > Políticas internas LATAM

Normativa PCI

Cuando una empresa ofrece la oportunidad de pagar con tarjetas de crédito o débito, significa que trabaja con datos sensibles que tienen que ser protegidos.

Los clientes deben sentirse seguros cuando pagan, por esto es que todos tenemos la responsabilidad de asegurar que las transacciones se realicen de una manera totalmente segura.

Normativa PCI

Payment Card Industry Data Security Standard (PCI DSS) es una norma de seguridad de datos de la industria de tarjetas de pago, desarrollada para fomentar y mejorar la seguridad de los datos de la tarjeta con dos objetivos principales:

- Evitar el fraude.
- Facilitar la adopción de medidas de seguridad uniformes a nivel global.

Normativa PCI

El cumplimiento de este estándar es tarea de todos, así como también el reportar en caso de detectar anomalías en el proceso.

Para esto te indicamos cuáles son los datos sensibles de las Tarjetas de Crédito que debemos cuidar:

Normativa PCI

- El Grupo LATAM posee un ambiente aislado, exclusivo para el manejo de datos de tarjetas de crédito. Este ambiente está compuesto de sistemas que soportan procesos de almacenamiento, transmisión y procesamiento de datos de tarjeta, así como los procesos y sistemas que protegen dicho ambiente.

- Almacenar, transmitir y/o procesar datos de tarjetas de crédito fuera del ambiente seguro es una violación grave a las políticas de seguridad del Grupo LATAM.

- Todos tenemos la responsabilidad de cuidar los datos de todos los clientes. Te invitamos a reportar a tu jefatura cuando veas que estos datos no se están manejando dentro de un ambiente seguro.

Seguridad de la Información

Módulo II

Protección de datos e información en dispositivos electrónicos del trabajo

¿Cuáles son las principales amenazas a la información?

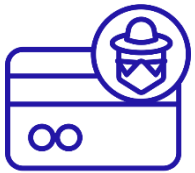
Actualmente las amenazas y ciberataques a empresas aumentan día a día, por este motivo, debemos comprometernos a protegernos de amenazas tales como:

ACCESO NO AUTORIZADO

MALWARE Y VIRUS

ROBO O FUGA DE DATOS

ATAQUES DE FUERZA BRUTA

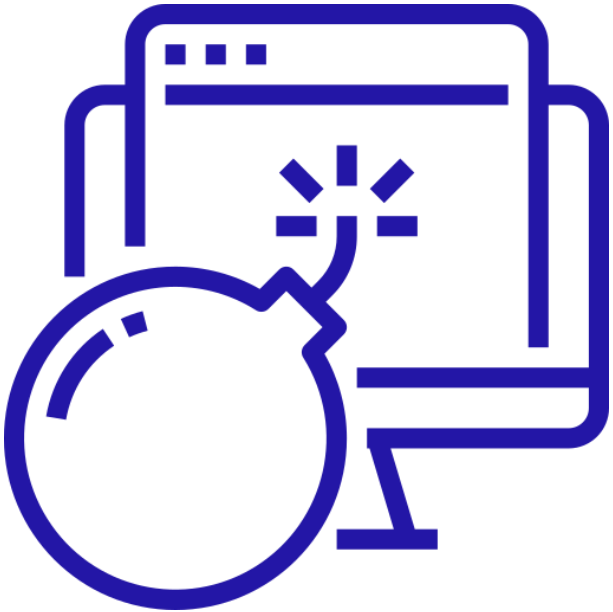


FRAUDE

¿Cuáles son las principales amenazas a la información?

Ciberataque:

Es un ataque a través de internet, por parte de una persona mal intencionada, con el objetivo de interrumpir, deshabilitar, destruir o controlar maliciosamente el ambiente (infraestructura, sistema o proceso), destruir la integridad de los datos o robar información.



Principales amenazas a la información

ACCESO NO AUTORIZADO

Ataque que tiene como finalidad acceder a sistemas y a informaciones de la compañía sin autorización.

MALWARE Y VIRUS

Malware: software malicioso que intenta invadir, adquirir información o deshabilitar ordenadores, sistemas informáticos, redes y dispositivos móviles.
Virus: tipo de malware cuyo objetivo es alterar el correcto funcionamiento de un dispositivo, infectando sus ficheros mediante un código maligno.

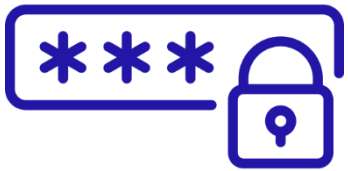
Principales amenazas a la información

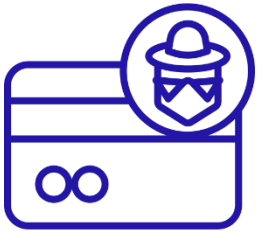
ROBO O FUGA DE DATOS

Liberación deliberada o involuntaria de información confidencial o sensible aun medio o a personas que no deberían conocerla.

ATAQUES DE FUERZA BRUTA

Método que permite la averiguación de una contraseña probando todas las combinaciones posibles hasta dar con la correcta.





FRAUDE

Ataque que busca explorar fallas y manipular datos o programas para la obtención de un lucro ilícito.

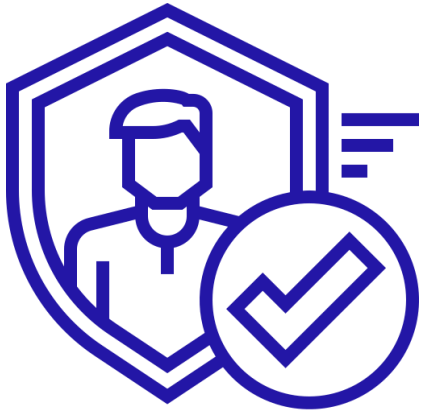
¿Cómo protegemos la información de la compañía?

Para proteger la información sensible de la compañía es necesario incorporar una serie de hábitos responsables:

- **Reflexionar sobre las acciones a seguir.**
- **Mantenerte actualizado.**
- **Contactar a los responsables de Seguridad de la Información.**
- **Usar tus redes sociales con precaución.**

Importante

Información sensible es toda información confidencial, restricta o información de identificación personal (IIP) que debe ser protegida y solo debe ser utilizada por personas autorizadas.



Por ejemplo:

Información financiera y de sueldos, datos estratégicos de la compañía, propiedad intelectual, información personal de clientes, empleados y proveedores que los identifiquen o que permitan identificarlos (como números de identificación personal, dirección, etc.).

Tips para proteger información sensible

Reflexiona sobre las acciones a seguir…

En cada actividad administrativa, operacional, reunión o proyectos en el que participes, reflexiona sobre qué acciones deberías seguir para garantizar que la información procesada esté segura.

Mantente actualizado

Infórmate sobre las directrices presentes en las políticas de seguridad de la información, boletines de seguridad y las normas relacionadas a tu actividad.

Tips para proteger información sensible

Contactar a los responsables de Seguridad de la Información

- Cuando empieces un proyecto, procura considerar las directrices de seguridad dela información relacionadas e involucra a los responsables de las políticas de seguridad de la información desde el principio.
- Cuando sospeches que eres víctima de un incidente o tengas dudas sobre las políticas y recomendaciones de seguridad, contacta de inmediato a los responsables de seguridad de la información.

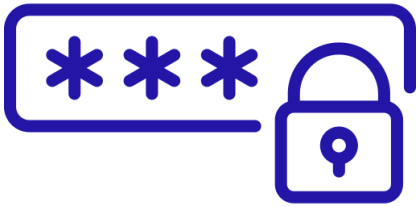
Tips para proteger información sensible

Usa tus redes sociales con precaución

- Evita publicar información personal o detalles que permitan identificar tu dirección (personal o laboral).
- Antes de compartir una información, verifica que no sea falsa (fake news).
- Antes de sincronizar tu cuenta a un aplicativo, revisa qué accesos se solicitan.
- Nunca realices publicaciones o declaraciones en nombre de la compañía.

¿Cómo proteger tu credencial corporativa?

La compañía establece una serie de requisitos que se deben tener en cuenta para crear una contraseña segura.



Recuerda que si sospechas que tu contraseña ha sido comprometida, cámbiala inmediatamente y reporta el incidente al área de responsable de seguridad de la información.

Adicionalmente, tu tarjeta de identificación física permite tu identificación dentro de la empresa, por lo que también es personal e intransferible.

Debes poner especial atención en siempre llevarla contigo.

¿Cómo crear una contraseña segura?

- Debe contar con una cantidad mínima de caracteres.
- Debe ser diferente de las últimas contraseñas utilizadas.
- Debe utilizar al menos una mayúscula, un número y un carácter especial (por ejemplo @, #, ^, (), _).
- Debe evitarse en uso de nombres, fechas, países.
- No compartir la contraseña con compañeros de trabajo.

¿Por qué es necesario cuidar nuestros dispositivos electrónicos?

Utilizar métodos de bloqueo en computadores y teléfonos celulares puede prevenir que personas mal intencionadas y ciberdelincuentes accedan a información relevantes de tu cuenta usando tu identidad.

Buenas prácticas de protección de dispositivos

PROTECCIÓN DE CREDENCIALES

- Asegúrate de que tu contraseña sea segura, que esté actualizada frecuentemente y que sea única para tu cuenta laboral.
- Recuerda que tus credenciales son personales e intransferibles. No deben ser compartidas no nadie.

PROTECCIÓN Y GUARDADO SEGURO DEL DISPOSITIVO

- Si tienes un computador portátil, usa un cable con candado de seguridad para restringirlo físicamente.
- Cuando salgas del trabajo al final del día, guarda tu computador portátil en zonas seguras con llave.

Buenas prácticas de protección de dispositivos

BLOQUEO DE PANTALLA

Siempre que dejes tu computador desatendido, bloquéalo de acuerdo a la combinación de teclas otorgada por tu empresa.

Por ejemplo: CTRL + ALT + SUPR

ACTUALIZACIÓN Y DESCARGA DE SOFTWARE

- No descargues archivos, software o aplicativos que no son autorizados y que no tienen licencia aprobada por la compañía.
- La instalación de software que viola derechos autorales y/o expone a la compañía a amenazas de ciberseguridad, como software de hacking es una violación a las políticas y estaría sujeta a gestión de consecuencias.

Buenas prácticas de protección de dispositivos

TRABAJO REMOTO

- Procura posicionar tu computador de modo que solo tu puedas visualizar la información en pantalla.
- Cuando utilices tu computador portátil fuera de la red de la compañía, verifica la posibilidad de usar una Virtual Private Network (VPN), que te proveerá de una conexión segura.

PROTECCIÓN DE DISPOSITIVOS MÓVILES

- Configura una contraseña segura para desbloquearlo y la compartas.
- Revisa la configuración de tus notificaciones, para que solo se puedan visualizar al desbloquear el dispositivo.

Buenas prácticas de protección de dispositivos

CUIDADO EN LA INSTALACIÓN DE APLICACIONES

- Antes de instalar una aplicación, revisa los permisos que se solicitan, como el acceso a tu correo, contactos, fotos, cámara, etc.
- Evita autorizar que la aplicación acceda a tu localización.

PROTECCIÓN Y GUARDADO SEGURO DEL DISPOSITIVO MÓVIL

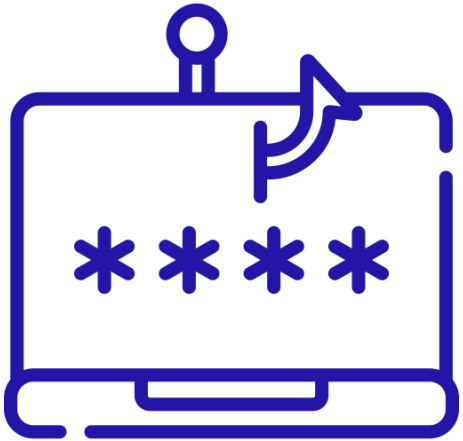
- Nunca dejes tu dispositivo desatendido, llévalo contigo o mantenlo en zonas seguras con llave.
- Nunca compartas tu dispositivo personal con nadie.
- Actualmente, los celulares son utilizados como un segundo control de seguridad para diferentes operaciones, como acceder a tus cuentas o realizar transacciones bancarias. Por eso es tan importante mantenerlo contigo y protegerlo.

¿Qué es una amenaza de ciberseguridad?

Son actos que pueden causar un daño grave a un activo o dispositivo digital. Pueden provocar ataques a dispositivos digitales, redes, datos y más.

- Todos los días utilizamos nuestras cuentas de correo para comunicarnos con nuestros colegas, proveedores y clientes.
- Evita utilizar tu cuenta de correo laboral para fines sociales y personales. Para esas instancias se recomienda el uso del correo personal.
- Por esto debemos estar atentos a las amenazas a las que estamos expuestos.

Principales amenazas



PHISHING

- Ataque de suplantación de identidad en el que un delincuente cibernético envía un correo electrónico o instant message que incluye un hipervínculo a un sitio peligroso.
- Generalmente, se ponen en práctica a través de campañas que solicitan una acción con urgencia, por ejemplo, promociones demasiado buenas para desaprovechar o notificaciones de que te ganaste un premio en un sorteo en el cual no participaste.

Principales amenazas

SPEAR PHISHING

- Ataque similar al phishing, pero más crítico, ya que es direccionado a una persona o área especifica.
- En este tipo de ataque, el atacante conoce al destinatario.

Principales amenazas

RANSOMWARE

- Ataque que tiene como objetivo secuestrar los datos de un usuario con el fin de solicitar el cobro de un rescate para poder acceder a ellos nuevamente,
- Este ataque normalmente es realizado a través de malware o virus instalado en el dispositivo.

Veamos algunos ejemplos…

Identifica cuál de los siguientes correos puede representar una amenaza para la seguridad de la información.

New Message (1 / 3)
***De**: beneficiosalpersona@tuempresa2.com*
***Para**: Paz Gaete*
***Asunto**: Salud y Bienestar – Nuevo Beneficio*
Como parte de las acciones de la empresa, para promover el bienestar y los hábitos saludables de todos los empleados, se ha establecido una nueva alianza con el Centro de Estética Integral (CEI). *Estamos muy contento de informarte que haz sido seleccionada para recibir un regalo sorpresa por parte nuestra.* *Para revisar el listado de regalos disponibles, haz clic aquí.* *Ingresa cuanto antes, el stock de cada producto es limitado.* *Beneficios al Persona.*

Este correo es seguro

Este correo es spam

New Message (2 / 3)
De: *francisca.godoy@tuempresa2.com*
Para: *Mario Sepúlveda*
Asunto: *Reporte de Status Semanal*
Buenos días Mario, *Me comunico para informarte que esta semana se sumó un nuevo colaborador al equipo y necesita acceso a la carpeta donde se alojan los reportes de status.* *Por favor, asígnale de inmediato permisos de edición a esta carpeta.* *Su correo es oscar.orozco@tuempresa2.com* *Saludos.* *Francisca.*

Este correo es seguro

Este correo es spam

New Message (3 / 3)
De: *mesa.ayuda@tuempresa2.com*
Para: *Juan Muñoz*
Asunto: *Casilla de correo sin espacio*
Estimado Juan, *Hemos detectado que su casilla de correo está próxima a llegar a su límite.* *La política de la empresa requiere resolver la situación de inmediato.* *Ejecute el archivo adjunto para que les comenten instrucciones detalladas sobre cómo proceder.* **`Instrucciones INBOX sin espacio.bat`**. *Mesa de Ayuda.*

Este correo es seguro

Este correo es spam

Buenas prácticas para el uso del correo

Al recibir un correo sospechoso

- Márcalo como SPAM (correo basura).
- Repórtalo al equipo responsable de seguridad de la información.

Al compartir un archivo

- Verifica a quién estás compartiendo esta información y si esa persona debería tener acceso a ella.
- Comparte información indicando la casilla de correo y no por vínculo directo.
- Otorga siempre el mínimo de privilegios necesarios.
- Otorga permiso de visualización por tiempo limitado.
- Comparte información solamente con usuarios de tu empresa.

Buenas prácticas para el uso del correo

Medios de almacenamiento seguro

- Toda la información de la compañía debe almacenarse en los repositorios autorizados.
- De acuerdo al tipo de datos y a los requerimientos específicos del área se podrá optar por un equipo servidor o por un sistema de almacenamiento web definidos por la compañía.

Mesas limpias

- Es necesario prestar atención al almacenamiento correcto de la información, principalmente cuando es confidencial.
- Recuerda siempre recoger tus reportes de la impresora de modo inmediato, mantén tu mesa limpia y cuando utilices pizarras en salas de reuniones, límpialas antes de salir.

Buenas prácticas para el uso del correo

Recomendaciones para el resguardo de la información

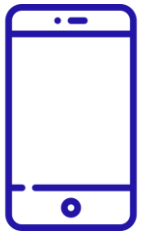
- Elimina completamente la información que ya no necesitas.
- Evita almacenar información personal en las estaciones de trabajo, notebooks, teléfonos dela empresa y en carpetas de red.
- Restringe el acceso a carpetas dela red y a documentos confidenciales.

Veamos algunos ejemplos…

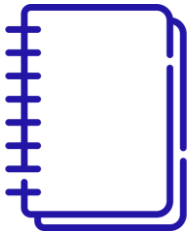
Identifica cuál de las siguientes alternativas es correcta para cada elemento.

Tarjeta de Identificación

Información del Cliente



Teléfono Móvil



Documentos Corporativos

Llevar consigo

Cajón con llave

Equipaje de viaje

Basurero

Trituradora de papel

Recuerda…

- Si crees haber sido víctima de una evento de seguridad de la información potencialmente peligroso para tu compañía no lo dudes.
- Comunícate al instante con el equipo responsable ante incidentes de seguridad de la información.
- Reportar el incidente a tiempo es imprescindible para que el equipo actúe, restituyendo las actividades con el mínimo de impacto posible.

Seguridad de la Información

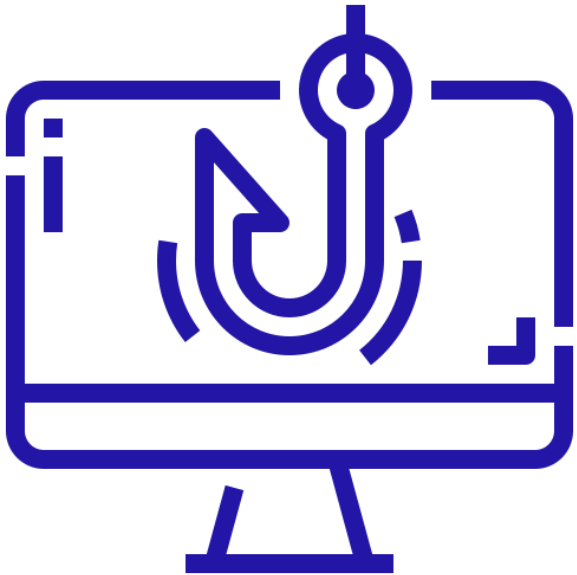
Módulo III

Protección de datos e información en dispositivos personales

¿Qué es la Ingeniería Social?

La Ingeniería Social es un método utilizado por los cibercriminales para manipular y engañar a sus víctimas con el fin de obtener información, cometer fraude o acceder ilegalmente a sus dispositivos.

Logran su cometido valiéndose de la confianza de las personas y mediante una estrategia dirigía de espionaje. Por eso, es fundamental que estemos alerta para resguardar nuestra información y la de la compañía.



Principales amenazas de la Ingeniería Social

- Al realizar compras por internet.
- Al enviar o recibir correos electrónicos.
- Al publicar información en redes sociales.
- Al hablar temas confidenciales en espacios públicos.

Principales amenazas de la Ingeniería Social

El mejor método de prevención es estar informados

Conocer el valor que tienen nuestros datos en internet y los peligros que corremos si un desconocido accede a ellos nos ayuda a ser más cautos y más difíciles de engañar.

¿Cuáles son las formas más frecuentes de ataque?

INTERNET

Los ataques más comunes se realizan vía correo electrónico, sitios web fraudulentos o perfiles falsos en las redes sociales.

LLAMADAS TELEFÓNICAS

El perpetrador realiza una llamada a la víctima haciéndose pasar por alguien más, como un técnico de soporte o un empleado de la misma organización.

¿Cuáles son las formas más frecuentes de ataque?

SMS

El delincuente envía un mensaje de texto a la víctima ofreciéndole una promoción o un servicio. Si la persona lo responde, puede revelar información personal, ser víctima de un robo o de una estafa más elaborada.

TRASHING

El delincuente busca información relevante en la basura, como agendas telefónicas, organigramas, agendas de trabajo o unidades de almacenamiento (USB).

Veamos un ejemplo…

Recibes la siguiente llamada:

“Buenos días Ricardo…

Me contacto desde el área de tecnología de tu empresa para informarte que hemos detectado un inconveniente en tu correo corporativo y necesitamos actuar la brevedad…

Por favor envía tus credenciales a la siguiente casilla de correo mesa.apoyotecnologica@tuempresa2.com”

¿Qué deberíamos hacer?

a) **Enviar mis credenciales**

b) **Reportar incidente**

c) **Terminar la comunicación**

Tips para estar protegidos

PROTEGE TUS CUENTAS CON CONTRASEÑAS FUERTES

- Usa una combinación de mayúsculas, números y caracteres especiales.
- Usa métodos de autenticación adicionales cuando sea posible.
- Usa una contraseña diferente para cada cuenta.

ASEGURA TUS DISPOSITIVOS PERSONALES

- Mantén tus sistemas operativos y softwares actualizados.
- Establece contraseñas seguras.
- Usa softwares antivirus.
- Compra dispositivos de fabricantes confiables.

Tips para estar protegidos

PROTEGE TUS DATOS MIENTRAS VIAJAS

- Nunca dejes tus dispositivos desatendidos.
- Busca siempre posicionarte de modo que nadie pueda mirar tu pantalla.
- Usa tu propio punto de acceso para conectarte a internet.
- Utiliza la configuración de firewall “red pública” si debes conectarte a una red desconocida.
- Usa protector de pantalla.

PREVIENE ATAQUES POR CORREO ELECTRÓNICO

- No hagas clic en enlaces ni descargues archivos adjuntos en correos sospechosos.
- Desconfía de solicitudes urgentes de información confidencial.
- Presta atención a errores de ortografía y gramaticales.
- Revisa la dirección web de los enlaces al pasar sobre ellos.
- Antes de ingresar información personal en internet, verifica que la dirección comience con “https://”.

Gracias

Capacitación Aeropuerto

REV.00 01.01.2021