LA SEGURIDAD EN LÍNEA ES RESPONSABILIDAD DE TODAS Y TODOS

ÍNDICE

INTRODUCCIÓN

El presente folleto tiene como finalidad proporcionar a todas y todos los integrantes de organizaciones de la sociedad civil información técnica sobre seguridad digital, así como herramientas especializadas para la identificación, prevención de riesgos y capacitación autónoma. Se busca ampliar el conocimiento y fortalecer las competencias de todas y todos en el uso de los medios digitales, haciendo énfasis en las posibles vulnerabilidades a las que pueden estar expuestos. Mantener una protección constante requiere un esfuerzo continuo, por lo que también se incluye un conjunto de contactos seguros que pueden asistir a todas y todos en diversos contextos.

GRUPO DE PENSAMIENTO AFRODESCENDIENTE

Promover la visibilización de los sectores históricamente excluidos y los grupos de atención prioritaria con énfasis en la población afrodescendiente. A través de la participación activa y efectiva en los procesos de desarrollo social, económico y político del país, bajo la articulación y promoción de acciones que contribuyen al crecimiento intelectual y bienestar de las y los ciudadanos como un aporte desinteresado con la educación y la cultura del Ecuador.

GPA
Grupo de Pensamiento Afrodescendiente

CONEXIÓN EDUCATIVA

Organización sin fines de lucro dedicada a promover los derechos humanos y la justicia social mediante el intercambio de conocimientos, la investigación y el acompañamiento en la implementación de tecnologías digitales responsables. Nos esforzamos por generar soluciones que no solo mejoren la calidad de vida, sino que también contribuyan a la protección del medio ambiente y a la construcción de un futuro más resiliente.

Conexión Educativa

SIEMPRE UTILIZA CONTRASEÑAS SEGURAS

Una contraseña segura es la primera barrera de defensa para proteger tu información personal en línea. Utilizar una combinación de letras mayúsculas y minúsculas, números y símbolos, así como evitar palabras comunes o datos personales, es clave para fortalecer la seguridad.

¿Qué debe tener una contraseña segura?

- Longitud mínima de 12 caracteres.
- Uso de caracteres especiales (@, #, $, %, etc.).
- Mezcla de mayúsculas, minúsculas y números.
- Evitar datos personales (nombres, fechas de nacimiento, etc.).
- No repetir contraseñas en diferentes plataformas.

Herramientas para gestionar tus contraseñas

Utilizar un gestor de contraseñas es una excelente forma de almacenar de manera segura tus claves. Existen herramientas tanto gratuitas como de pago que pueden ayudarle a generar y guardar contraseñas seguras. Entre las más recomendadas están:

Proton Pass: Una aplicación móvil gratuita que almacena de forma segura todas tus contraseñas y genera claves fuertes para tus cuentas.

KeePass: Es un software libre para la gestión de contraseñas y puede usarse en dispositivos android y ordenadores.

SEGUNDO FACTOR DE AUTENTICACIÓN (2FA)

Estas opciones refuerzan significativamente la seguridad de tus cuentas al agregar una segunda capa de protección, incluso si alguien obtiene tu contraseña.

Códigos SMS: Tras ingresar tu contraseña, recibirás un código temporal por mensaje de texto que deberás introducir para completar el inicio de sesión. Aunque es fácil de usar, ***no es el método más seguro.***

Aplicaciones de autenticación: Generan códigos temporales de un solo uso, proporcionando mayor seguridad que los SMS.

Llaves de seguridad física: Dispositivos como YubiKey se conectan a tu computadora o teléfono y se usan para confirmar tu identidad. Ofrecen uno de los niveles más altos de protección.

HABLEMOS DE PHISHING

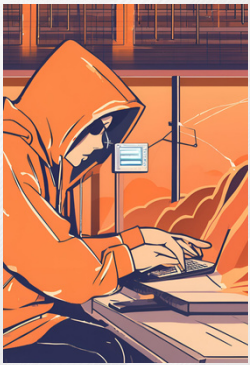
Es una técnica de estafa en la que los delincuentes se hacen pasar por entidades confiables para obtener información confidencial, como contraseñas o datos personales, que luego utilizan para extorsión, robo de dinero o suplantación de identidad.

¿Cómo reconocer el phishing?

Saludos genéricos: Mensajes como "Estimada/do cliente" son sospechosos.

Solicitud de información personal: Los bancos rara vez piden datos confidenciales por correo, WhatsApp u otros medios.

Correspondencia inesperada: Contactos no solicitados de bancos o servicios en línea son inusuales.

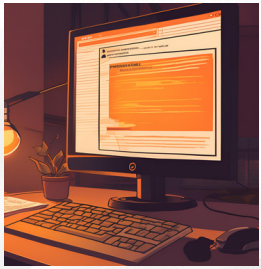


Urgencia: Los mensajes que te presionan a actuar rápidamente son señales de alarma.
Ofertas demasiado buenas: Si parece increíble, probablemente sea una estafa.
Dominio sospechoso: Correos de dominios no oficiales o extranjeros.

Protégete del Phishing:

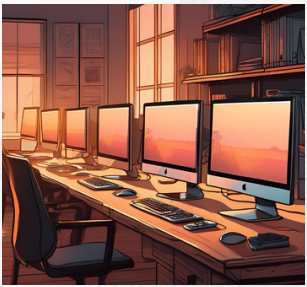
- No compartas tu información personal a través de enlaces en correos sospechosos.
- **Verificación de links:** Para verificar que un link no sea malicioso se puede utilizar:
  - https://phishtank.org/
  - https://www.shouldiclick.org/
- Mantén actualizado tu antivirus.
- Utiliza autenticación de dos factores para mayor protección.

RECOMENDACIONES PARA COMPUTADORAS



- **Identifica tus datos críticos:** Define información esencial que merece protección.
- I**mplementa la estrategia 3-2-1:** 3 copias de tus archivos en 2 tipos de almacenamiento diferentes, con 1 copia en una ubicación externa.
- **Elige el almacenamiento adecuado:** Usa discos duros externos, dispositivos NAS o servicios en la nube.

NAS: dispositivo de almacenamiento en red que permite el acceso colaborativo y centralizado a archivos.



- **Programa y automatiza copias de seguridad:** Establece un calendario regular.
- **Prueba la recuperación de datos:** comprueba la restauración regularmente.
- **Documenta y capacita:** Registra tu estrategia y enseña a otras y otros.

RECOMENDACIONES PARA MÓVILES

- **Mantén el sistema operativo y las aplicaciones actualizadas:** Asegúrate de instalar las últimas actualizaciones para protegerte contra vulnerabilidades.
- **Usa contraseñas fuertes y autenticación de dos factores:** Protege tu dispositivo con contraseñas robustas y activa la autenticación en dos pasos para mayor seguridad.
- **Evita redes Wifi públicas no seguras:** Cuando estás en lugares públicos, usa una VPN para navegar de forma segura y proteger tus datos.

VPN(Virtual Private Network): Es un tunel seguro para conectarte a internet, te brinda privacidad al cifrar tu conexión y cambiar tu dirección IP real.

- **Sé cautelosa/so con los enlaces y descargas:** No hagas clic en enlaces sospechosos ni descargues archivos de fuentes no confiables.
- **Realiza copias de seguridad regularmente:** Asegúrate de respaldar tus datos de forma automática para no perder información importante.
- **Usa la función de bloqueo remoto y borrado.**

TEST DE SEGURIDAD DIGITAL

Responde a las interrogantes con sinceridad, toma en cuenta las siguientes consideraciones: **A** es Siempre, **B** es Rara vez y **C** es Nunca

¿Tienes activada la autenticación de dos factores (2FA) en tus cuentas más importantes?

○ **A** ○ **B** ○ **C**

¿Lees las políticas de privacidad antes de descargar aplicaciones?

○ **A** ○ **B** ○ **C**

¿Sueles abrir correos electrónicos de remitentes que no conoces?

○ **A** ○ **B** ○ **C**

¿Evitas conectarte a redes Wifi públicas sin protección?

○ **A** ○ **B** ○ **C**

¿Actualizas regularmente el software y las aplicaciones en tus dispositivos?

○ **A** ○ **B** ○ **C**

TEST DE SEGURIDAD DIGITAL

¿Usas contraseñas diferentes para cada cuenta en línea?

A B C

¿Con qué frecuencia cambias tus contraseñas?

A B C

¿Tus dispositivos tienen un software antivirus actualizado?

A B C

¿Descargas aplicaciones y archivos solo de fuentes confiables?

A B C

Resultados:
Mayoría A): ¡Felicidades! Tienes buenos hábitos de seguridad digital.
Mayoría B): Tu seguridad digital es moderada, pero podrías mejorar.
Mayoría C): Estás en riesgo.
¡Es hora de reforzar tu seguridad en línea!

PRÁCTICAS SEGURAS

En el mundo digital actual, es fundamental estar preparada/do para proteger tu información y mantenerte segura/ro en línea. Te presentamos algunas soluciones esenciales que te ayudarán a prevenir incidentes informáticos y crear un entorno seguro para ti y las/los tuyos.

Shira

Es una herramienta diseñada para desarrollar tus habilidades en la identificación y prevención de ataques de phishing. Te enseñará a reconocer correos y mensajes sospechosos, ayudándote a evitar robos de información personal.

Kit de Primeros Auxilios Digitales

Este recurso te guía en la protección frente a problemas de seguridad digital, ayudándote a diagnosticar incidentes y conectándote con soporte especializado para una solución más detallada.

DIGITAL FIRST AID KIT

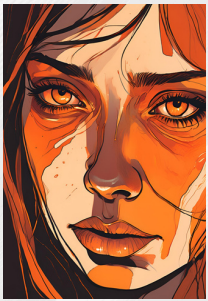
GESTIÓN EMOCIONAL EN INCIDENTES

Ser hackeada/do o caer en un ataque de phishing puede provocar una variedad de emociones intensas. Aquí algunas de las emociones más comunes que puedes presentar: Miedo, ansiedad, frustración, ira, vergüenza, culpa, confusión, estrés.

Recomendaciones:

Reconoce tus emociones:
Date permiso para procesar esas emociones sin juzgarte.

Busca apoyo:
Hablar con alguien de confianza, puede ayudar a aliviar el estrés. Si la ansiedad es demasiado abrumadora, considera buscar ayuda profesional.



Mantén la calma y toma control:
Cambia tus contraseñas, informa el incidente a las autoridades o servicios de soporte, y activa medidas de seguridad adicionales.

Evita la autocrítica:
Cualquiera puede ser víctima de un ataque. Culparte solo aumentará el malestar emocional, concéntrate en aprender de la experiencia.

Empodérate con conocimiento:
Investigar sobre cómo protegerte mejor podrá aliviar la sensación de vulnerabilidad.

Ser víctima de un hackeo puede afectar tus emociones, pero con el enfoque adecuado y las medidas de apoyo, puedes superar el impacto y mejorar tu resiliencia.

CONTACTOS SEGUROS

Línea de Ayuda - Incidentes informáticos

Ofrece soporte gratuito y accesible a personas de la sociedad civil, con especial atención a comunidades afrodescendientes, pueblos indígenas, activistas, comunicadores populares y miembros de la comunidad LGBTIQ+.

Conexión Educativa

Escribenos a:

@ayudaConexionEduEc_bot
ayuda@conexioneducativa.org
0984290670

Fondo de Respuesta Rápida - FRR

Ayuda en la protección de derechos digitales en América Latina (FRR) brinda apoyo a activistas y organizaciones de la sociedad civil enfrentados a emergencias que no pueden ser satisfechas por los ciclos de financiamiento tradicionales.

FONDO DE RESPUESTA RÁPIDA
para la protección de derechos digitales en América Latina

frr@derechosdigitales.org
PGP Fingerprint
7BB4 86B0 79C2 47F6 3756 5CA8 A46B 6570 AB3B 8C47

Línea de ayuda de Access Now

Trabaja con individuos y organizaciones de todo el mundo para mantenerlos seguros en línea. Si ya estás bajo ataque, proporciona asistencia de emergencia de respuesta rápida. Servicios disponibles las 24 horas, los 7 días de la semana y en 8 idiomas diferentes.

accessnow

www.accessnow.org
help@accessnow.org
PGP Fingerprint:
6CE6 221C 98EC F399 A04C 41B8 C46B ED33 32E8 A2BC

Glosario

- **NAS (Network Attached Storage):** Es un dispositivo que se usa para guardar archivos y compartirlos fácilmente entre varias computadoras en una misma red, como si fuera un gran disco duro al que todos pueden acceder.
- **PGP (Pretty Good Privacy) Fingerprint:** Es una especie de "huella digital" que se usa para confirmar que un mensaje o archivo realmente viene de quien dice ser. Ayuda a garantizar que la comunicación sea segura y no haya sido alterada.
- **VPN (Virtual Private Network):** Es un servicio que te permite conectarte a internet de forma más segura. Es como si crearas un túnel privado que protege todo lo que haces en línea, manteniendo tus datos seguros y ocultos.
- **Llaves de seguridad física:** Son pequeños dispositivos que se conectan a tu computadora o teléfono para confirmar tu identidad. Funcionan como una llave extra para tus cuentas, brindándote una capa adicional de protección.
- **Antivirus:** Es un programa que revisa tu computadora o teléfono para detectar y eliminar virus u otros programas maliciosos que puedan dañarlo. Es importante tener un antivirus para mantener tus dispositivos protegidos y seguros.

SEGURIDAD DIGITAL

GPA
Grupo de Pensamiento Afrodescendiente

@gpafroficial

Conexión Educativa

@conexioneduec

CON EL APOYO DE:

FONDO DE RESPUESTA + RÁPIDA
para la protección de derechos digitales en América Latina