Seguridad digital y gestión del riesgo

Sesión #3: Buenas prácticas

2025

Funded by the European Union

¿Seguridad digital? ¡Yo de eso no sé!

Pensemos cómo protegernos en medios digitales

Seguridad digital y análisis de riesgo

Introducción a la Seguridad digital para Organizaciones No Gubernamentales (ONG) y defensores y defensoras de Derechos Humanos (DDHH)

Comprender el entorno digital, las actoras y los actores presentes y las amenazas que enfrentamos en él.

1

2

Hay que cuidar las comunicaciones

Decidir qué herramientas usar y cómo configurarlas para mejorar la seguridad y la privacidad.

Mejores prácticas digitales

Construir un plan de mejora que incluya mejores prácticas y compromisos de uso.

3

Sesión #3: Buenas prácticas

Objetivos

- ¿Qué sabemos de nuestras propias vulnerabilidades y capacidades de respuesta?
- ¿Cuáles son las más básicas buenas prácticas que debemos implementar en nuestra ONG?
- ¿ Desarrolla y evalúa un plan de respuesta los incidentes cibernéticos?

Repasemos los conceptos del análisis de riesgo

La búsqueda de equilibrio...

Buenas prácticas

Riesgos
Ataques
Vulnerabilidades

RECORDATORIO

Riesgos digitales

Lo que no queremos que pase

- Pérdida de acceso a una cuenta
- Pérdida de información
- Pérdida del equipo
- Acceso no autorizado a información
- Sobreexposición de información personal
- Exponer a tus fuentes

Ataques frecuentes

Cómo actúan nuestros adversarios

- Phishing
- Explotación de vulnerabilidades
- Doxxing
- Spyware
- Chantaje
- Acoso en línea
- Amenazas en línea
- Violencia de género facilitada por la tecnología

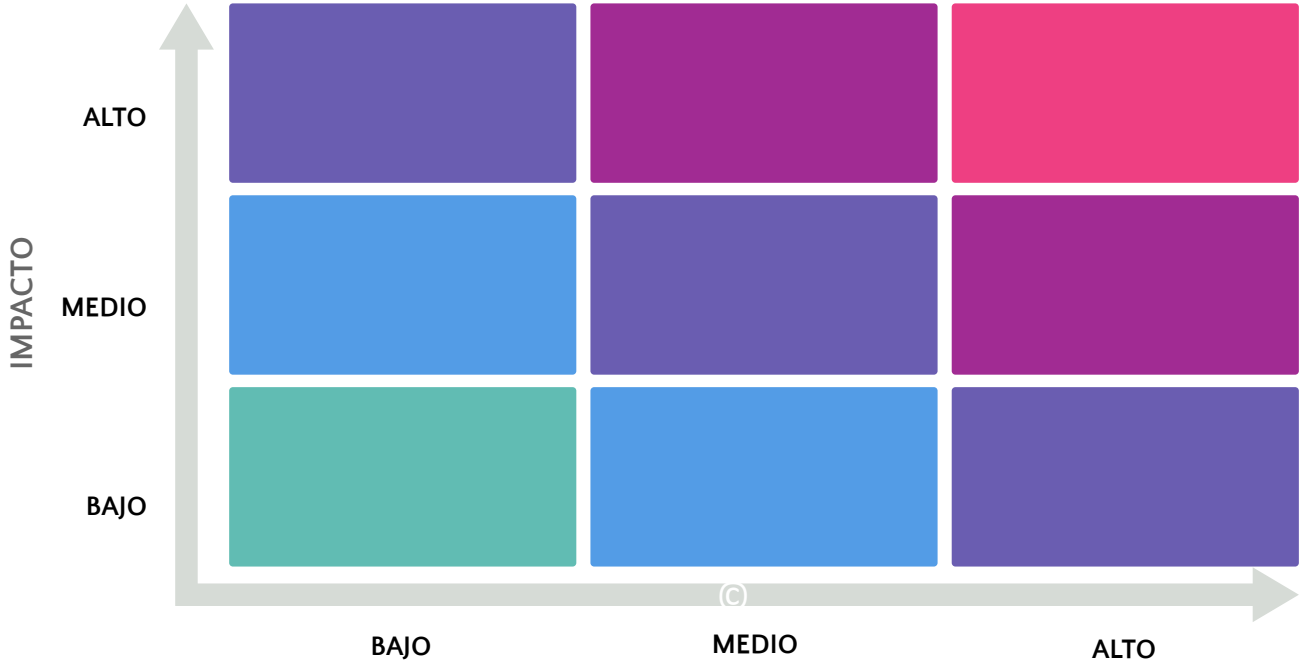
Vulnerabilidades

Algunas cosas que nos ponen en riesgo

- Usar malas contraseñas
- No bloquear los equipos
- No usa 2FA
- Abrir adjuntos desconocidos
- No tener copia de respaldo
- No actualizar los programas
- Usar redes públicas
- Usar aplicaciones de comunicación inseguras

Actividad 1

Breve ejercicio de análisis priorización de riesgo y ataques



Buenas prácticas

Cosas que equilibran la balanza

- ➔ Usar contraseñas únicas y fuertes
- ➔ Proteger dispositivos con contraseñas de inicio
- ➔ Usar 2FA en todas las cuentas
- ➔ Desconfiar de adjuntos desconocidos
- ➔ Respaldar periódicamente
- ➔ Configurar tu privacidad
- ➔ Mantener actualizaciones al día
- ➔ Cifrar todo lo que puedas cifrar
- ➔ Usar solo redes de confianza
- ➔ Usar aplicaciones de comunicación seguras
- ➔ Antivirus
- ➔ Seguridad perimetral

Actividad 2

Breve ejercicio de análisis de riesgo y ataques - identificación de buenas prácticas

Riesgo o ataque	Vulnerabilidades asociadas	Buenas prácticas de mitigación

Análisis de riesgo

Hacer que el esfuerzo valga la pena

El análisis de riesgo es una gran herramienta para encontrar los temas que debemos priorizar, pero la forma como debemos manejar los riesgos y posibles ataques dependerá de la disposición para mitigar las vulnerabilidades y de la capacidad de integrar buenas prácticas entre las personas de la organización y la propia organización.

Análisis de riesgo

Hacer que el esfuerzo valga la pena

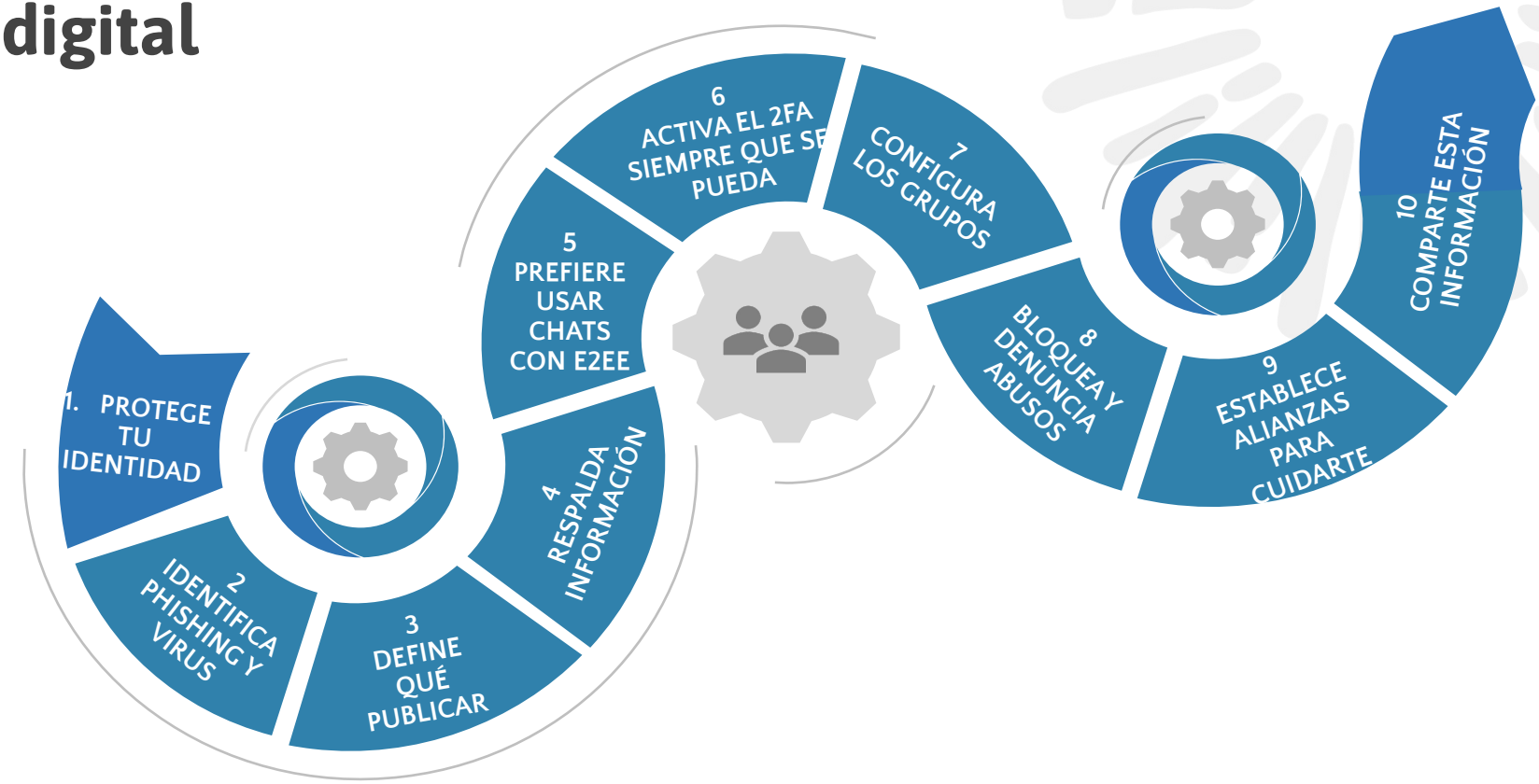
Con un análisis de riesgo es posible hacer un plan de mejora, para lo que deben:

- Ser realistas sobre los recursos y las capacidades de la organización,
- Buscar ayuda en otras organizaciones,
- Asignar recursos y tiempos para las tareas pendientes,
- Realizar un seguimiento continuo.

La seguridad digital es un proceso en el cual aprendemos a tomar mejores decisiones y desarrollamos un espíritu crítico y reflexivo sobre la tecnología.

Un camino posible

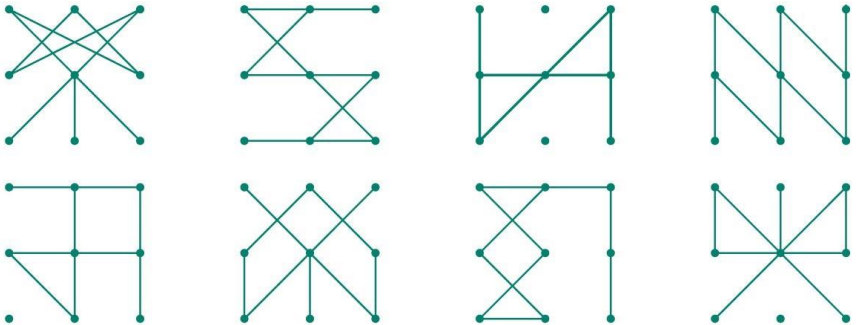
10 pasos para mejorar nuestra seguridad digital



10 recomendaciones básicas

1. Celulares

- Con buena clave o patrón.
- La huella o la cara no están mal como seguridad pero revelan mucha información.
- Hacer copias de seguridad.
- Siempre que se pueda, cifrar el teléfono completamente.



2. Computadores de terceros.

Cafés internet - espacio público - el computador de otra persona

- Usar modo incógnito.
- Borrar archivos descargados.

3. Herramientas seguras

- Evitar llamar y enviar SMS por la red celular.
- Mejor usar WhatsApp.
- **Muuucho mejor usar Signal.**
- Persuadir a los contactos de usar sistemas más seguros de comunicación es importante.

4. Navegación en internet.

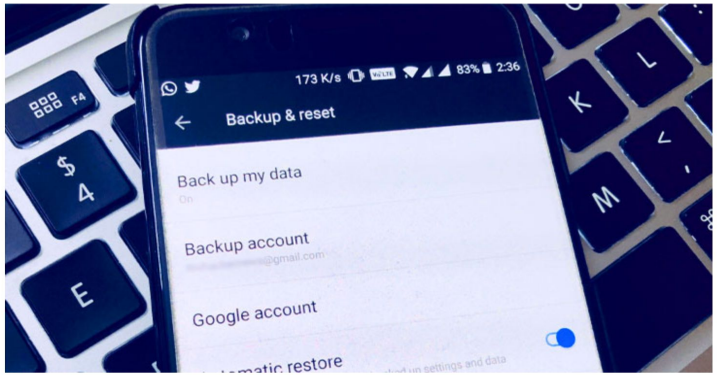
- Revisar configuración de seguridad del navegador.
- Deshabilitar sistemas de rastreo como las cookies de terceros.
- Borrar historiales de navegación comprometedores.
- Mantener el navegador actualizado.
- De acuerdo a las circunstancias usar VPN o TOR.

5. Copias de respaldo.

- Backup, backup, backup
- Cifrar, cifrar, cifrar.

Google to Encrypt Android Cloud Backups With Your Lock Screen Password

October 15, 2018 Swati Khandelwal



In an effort to secure users' data while maintaining privacy, Google has announced a new security measure for Android Backup Service that now encrypts all your backup data stored on its cloud servers in a way that even the company can't read it.

Ejemplos de formas de hacer copias de respaldo.

VeraCrypt

Google Drive

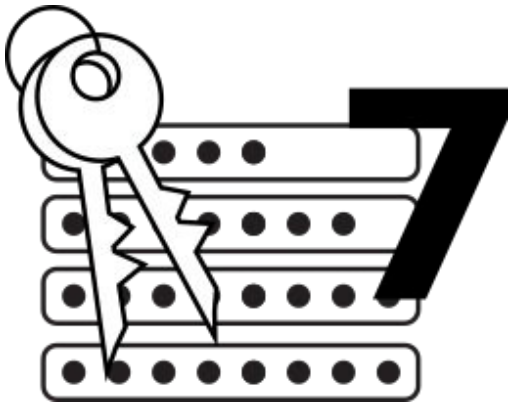
iCloud

One Drive

6. Publicaciones en internet.

- Procurar no hacer público:
  - Información personal.
  - Números de identificación
  - Teléfonos
  - Direcciones
  - Ubicación
- Ojo con etiquetar personas o con las etiquetas en general.
- Establecer con cuidado quienes pueden ver o no cada publicación.

7. Contraseñas.



- Contraseñas largas y complejas (números, letras, mayúsculas minúsculas).
- Procurar no repetir contraseñas entre cuentas.
- Cambiarlas de vez en cuando.
- Si inevitablemente se debe poner una contraseña en el computador de un tercero, cambiarla lo más pronto posible.
- Opcional: Usar un gestor de contraseñas como KeePassXC

8. Información sensible.

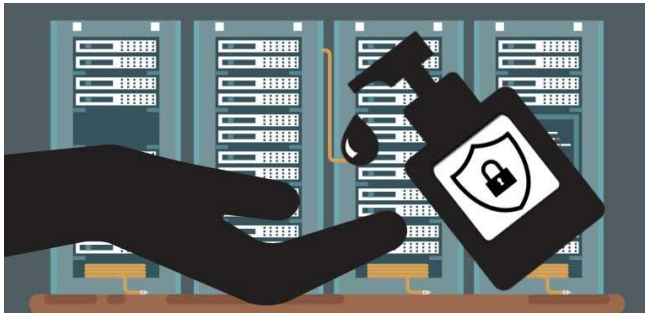
- ¿Por dónde viaja?
- ¿Dónde queda almacenada?
- ¿Quién puede tener acceso a ella?

- Cifrar, cifrar, cifrar.
- PGP, 7-Zip, Veracrypt.

9. Proteger cuentas en redes sociales.

- Contraseñas seguras
- Para fanpages o donde se pueda asignar roles (administrador, editor, moderador, etc) y permisos.
- Habilitar autenticación de dos pasos (2FA) con autenticadores como Authy o Google Authenticator en vez del número de teléfono para evitar el sim swapping y backup.

10. Ciber Higiene



- Cuidarse en internet y en el mundo real
- Mantener sistemas operativos y software actualizados.
- Revisar configuraciones de seguridad y privacidad con regularidad.
- Limpiar la casa (borrar software viejo o que no se usa, borrar archivos viejos o innecesarios).

¡Gracias!

www.innovusconsulting.co

Personas facilitadoras de la sesión: Catalina Valenzuela, Paula Quiñones y Camilo Forero

Creadora del módulo: Carolina Botero