Seguridad digital y gestión del riesgo

Sesión #1: Introducción a la seguridad digital para Organizaciones No Gubernamentales (ONG) & defensores y defensoras de derechos humanos (DDHH)

2025

AFD Agence Française de Développement
Funded by the European Union
forus Connect Support Influence
INNOVUS

¿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 #1: Introducción a la seguridad digital para Organizaciones No Gubernamentales (ONG) & defensores y defensoras de Derechos Humanos (DDHH)

Objetivos

- Identificar cómo funciona internet y el rol de las empresas intermediarias.
- Identificar las herramientas digitales que más usamos.
- Identificar los riesgos, amenazas, vulnerabilidades y capacidades que las ONG y defensores y defensoras de DDHH enfrentan en el uso de tales herramientas.

La seguridad digital es un trabajo de colaboración y responsabilidad compartida

1. Cómo funciona internet

¿Cuántas empresas se necesitan para que funcione el correo?

Los intermediarios de internet

- Internet es un espacio que en principio se pensó **descentralizado**, **abierto** y **neutro**.
- Internet ahora es un **espacio dominado** por pocas grandes empresas tecnológicas (Alphabet, Amazon, Meta, Apple, Microsoft) que **definen la vida digital** de miles de millones de personas.
- Es necesario **entender cómo funciona internet** para **acordar usos** y **prácticas** desde los **contextos** de nuestras organizaciones y sus **necesidades**

Internet es un espacio que podemos usar para nuestros activismos

Actividad 1

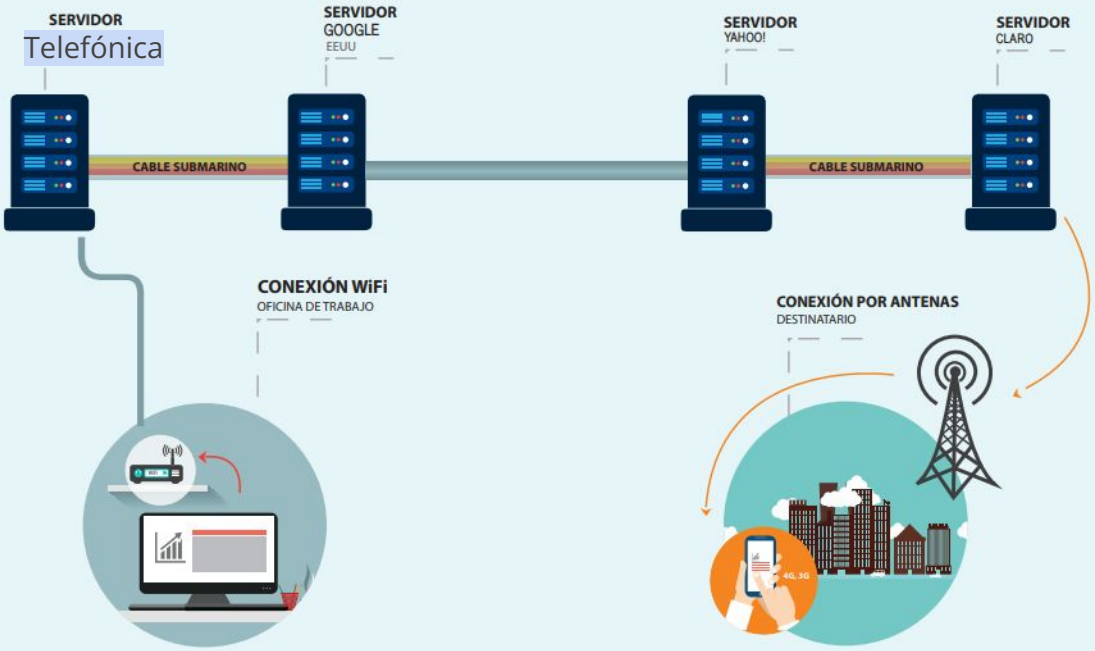
Enviemos un correo

Imaginemos que Ana envía un correo electrónico a Juan desde su portátil conectado por WiFi a un router de Telefónica. Ella usa un correo de Google. Juan usa una cuenta de Yahoo! y lee el correo en su celular, que está conectado con un plan prepago de Claro.

¿Qué empresas intermediarias reconocemos?

¿Cómo se comunican entre ellas?

¿Qué dispositivos entran en juego?


SERVIDOR
Telefónica
SERVIDOR
GOOGLE
EEUU
SERVIDOR
YAHOO!
SERVIDOR
CLARO
CABLE SUBMARINO
CABLE SUBMARINO
CONEXIÓN WiFi
OFICINA DE TRABAJO
CONEXIÓN POR ANTENAS
DESTINATARIO
4G, 3G

¿Cuántas empresas se necesitan para que funcione el correo?

Empresas intermediarias de internet

- Existen diferentes tipos de intermediarias
  - Proveedores de acceso
  - Manufacturadores de hardware
  - Proveedores de nombre de dominio
  - Proveedores de hosting
  - Buscadores
  - Creadores de contenidos
  - Redes sociales
  - Comercio electrónico
  - Proveedores de analítica web y vigilancia
- En cada actividad que desarrollamos en internet intervienen múltiples empresas
- La seguridad nuestra y de nuestra información depende de esas empresas y de nuestras decisiones

Reflexionemos sobre nuestra relación con estas empresas

2. Inventario

¿Qué aplicaciones y servicios usamos cotidianamente?

Nuestro ecosistema digital

- La **experiencia** en el espacio digital es única y depende de nuestros **contextos**, **necesidades** y **prácticas** de uso.
- Es posible hablar de grados de **apropiación digital**
  - No usuarios o usuarias
  - Básico: Comunicación y entretenimiento
  - Intermedio: Educación y participación
  - Avanzado: Transacciones y usos sofisticados (Realizar eventos en línea, Investigar, descargar y configurar programas, realizar transferencias a terceras partes)
- Para usos básicos e intermedios es posible **definir tendencias** y proponer **mejores prácticas** de uso. Para usos avanzados es bueno pensar en **protocolos**.

Actividad 2

Hagamos un inventario de las principales aplicaciones que usamos en el trabajo

Comunicaciones (int)

Productividad (int)

Participación (ext)

¿Qué aplicaciones y servicios usamos cotidianamente?

Nuestro ecosistema digital

- Tener prácticas seguras requiere hablar francamente de nuestros usos, reconocer qué estamos haciendo bien, qué podría mejorar y cambiar algunos hábitos.
- La seguridad digital es un proceso en el cual aprendemos a tomar mejores decisiones y desarrollamos un espíritu crítico y reflexivo sobre la tecnología.
- En una organización, la seguridad depende de todos y todas.
- Lo mejor será estar preparados para los eventuales problemas y aprender de los incidentes.

Podemos crear una cultura de seguridad digital de la que todas las personas hagan parte.

3. Análisis de riesgo

La búsqueda de equilibrio...

Buenas prácticas

Riesgos
Ataques
Vulnerabilidades

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

¿Cuáles de estos riesgos han enfrentado ya?, ¿cómo lo manejaron? y ¿qué consecuencias tuvo?

¿Cuál riesgo de estos tememos más? y ¿por qué?

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

¿Cuáles de estos ataques hemos enfrentado ya?, ¿cómo lo manejaron? y ¿qué consecuencias tuvo?

¿A cuál ataque de estos tememos más? y ¿por qué?

Vulnerabilidades

Algunas cosas que nos ponen en riesgo

- ➔ Usar malas contraseñas
- ➔ No bloquear los equipos
- ➔ No usar 2FA
- ➔ Abrir adjuntos desconocidos
- ➔ No tener copia de respaldo
- ➔ No actualizar los programas
- ➔ Usar redes públicas
- ➔ Usar aplicaciones de comunicación inseguras
- ➔ No actualizar el sistema operativo del computador

¿Cuáles de estas vulnerabilidades reconocemos?,

¿hay alguna que no puedan cambiar? y ¿por qué?

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

¿Hay alguna buena práctica de este listado que quieran implementar?

¿Alguna que quieran agregar?

Glosario

Análisis de riesgo: El análisis de riesgo, también conocido como evaluación de riesgos o PHA por sus siglas en inglés. Process Hazards Analysis, es el estudio de las causas de las posibles amenazas y probables eventos no deseados y los daños y consecuencias que éstas puedan producir.

Intermediario de internet: Un intermediario de internet se refiere a una empresa que facilita el uso de internet . Entre estas empresas se incluyen los proveedores de servicios de internet (ISP), los motores de búsqueda y las plataformas de redes sociales.

Phishing: es un término informático que distingue a un conjunto de técnicas que persiguen el engaño a una víctima ganándose su confianza haciéndose pasar por una persona, empresa o servicio de confianza (suplantación de identidad de tercero de confianza), para manipularla y hacer que realice acciones que no debería realizar (por ejemplo, revelar información confidencial o hacer click en un enlace).

Explotación de vulnerabilidades. Las vulnerabilidades son fallos en los sistemas computacionales que pueden ser aprovechadas (explotadas) por un atacante para realizar acciones no autorizadas que pueden comprometer la seguridad de la información contenida en los sistemas o el funcionamiento mismo de dichos sistemas.

Doxxing: Los términos doxing, doxxing y doxeo[1] (adaptación al español) describen el acto de revelar intencional y públicamente información personal sobre un individuo u organización, generalmente a través de internet.[

Spyware: El programa espía (en inglés spyware) es un malware que recopila información de una computadora y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del computador.

Chantaje; Un chantaje es la amenaza de difamación pública o daño semejante para obtener algún provecho pecuniario o material de alguien u obligarlo a actuar de una determinada manera. El chantaje o extorsión es un delito en el ordenamiento jurídico de muchos países

Acoso en línea; El ciberacoso o acoso cibernético (derivado del término en inglés cyberbullying), también denominado acoso virtual, es el uso de medios digitales para molestar o acosar a una persona o varias personas mediante ataques personales, divulgación de información personal o falsa entre otros medios. Los actos de ciber agresión poseen unas características concretas que son el anonimato del agresor, su velocidad y su alcance..

Amenazas en línea: también conocida como ciberamenaza, es cualquier acto malicioso que busca comprometer la seguridad de sistemas informáticos, redes o dispositivos, con el fin de obtener acceso no autorizado, robar datos, causar daños o interrumpir operaciones.

Violencia digital de género, también conocida como violencia de género facilitada por la tecnología, se refiere a cualquier acto de violencia que ocurre en línea y que se dirige a personas por razones de género. Esta violencia se manifiesta a través de diversos medios digitales, como redes sociales, teléfonos móviles, plataformas de internet, y puede incluir acoso, amenazas, difusión de contenido íntimo sin consentimiento, entre otros.

¡Gracias!

www.innovusconsulting.co

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

Creadora del módulo: Carolina Botero