AFD AGENCE FRANÇAISE DE DÉVELOPPEMENT

Funded by the European Union

forus CONNECT SUPPORT INFLUENCE

INNOVUS

Seguridad digital y gestión del riesgo

Sesión # 3

Buenas prácticas

2025

1. Información General

1. Nombre del curso/taller: Introducción a la Seguridad Digital para Organizaciones No Gubernamentales (ONGs) & defensores y defensoras de Derechos Humanos (DDHHs)
2. Duración: máximo 90 minutos
3. Público objetivo: directores de ONGs y organizaciones de derechos humanos
4. Objetivos del curso: Adquirir conocimientos básicos de seguridad digital para integrar a las prácticas cotidianas de las ONGs y organizaciones de derechos humanos que les permita fortalecer su capacidad de resiliencia y sostenibilidad.

2. Preparación para la facilitación

- Materiales necesarios: La presentación, no se necesita conocimiento previo, excepto haber diligenciado la encuesta. Para esta sesión en todo caso la persona que facilita la sesión deberá enviar a los correos de las personas que asistan las diapositivas 7, 8, 9 y 10 (lo puede hacer creando un archivo ppt con esas dos diapositivas). La idea es que durante la sesión, cuando se llegue al momento de desarrollar esa actividad cada persona pueda tener a mano y editar ese archivo y quedarse con su propia versión del análisis de riesgo y su forma de mitigación.
- Configuración del espacio: revisar el sonido, la imagen, poner la cortina del proyecto. Asegurarse que la posibilidad de crear grupos está habilitada y definir cómo se conformarán los grupos (al azar o lista predeterminada).
- Tecnologías de apoyo : enlaces, actividades y evaluación
- Preparación previa a la sesión (logística, revisión de materiales): Nada, sin embargo no olvide enviar la diapositiva 8
- Guía paso a paso para cada actividad: se encuentra en cada punto
- Indicaciones sobre transiciones entre temas: Están marcadas en la presentación
- Puntos críticos a enfatizar: Tener siempre presente que esto es un abrebocas y que no hay seguridad digital efectiva al ciento por ciento.

3. Guión de la sesión 2 (descrita dispositiva por dispositiva)

Minuto 1.	**Actividad/Acción de la persona facilitadora** Bienvenida y .presentar objetivos del curso	**Estrategia/Metodología** Relato sobre una visual genérica

Guión/instrucciones

- Bienvenida al curso Introducción a la Seguridad Digital para Organizaciones No Gubernamentales (ONGs) y de Derechos Humanos (DDHH)
- Nombre del facilitador: xxxxx
- No se requieren conocimientos previos para atender esta sesión, basta con haber diligenciado el cuestionario de construcción de la línea base.

Minuto 2.	**Actividad/Acciónde la persona facilitadora**	**Estrategia/Metodología**
	Introducción al tema	Relato sobre una visual genérica

Guión/instrucciones

- Entramos en nuestra tercera y última sesión sobre seguridad digital con un enfoque de análisis de riesgo. Esperamos que para este momento del curso puedan decir que han adquirido conocimientos básicos del tema y que tienen nociones y, especialmente nuevas herramientas, para cómo protegerse cuando habitan y usan medios digitales.
- Reiteramos que gracias a que las personas mejoran sus conocimientos en seguridad digital es que pueden usar la tecnología de forma segura, privada y con confianza. Es importante reiterar una vez más que una visión balanceada de la seguridad digital pone a las personas en el centro.
- ¡Empecemos!

Minuto 3	**Actividad/Acción de la persona facilitadora**	**Estrategia/Metodología**
	Introducción al tema	Relato sobre una visual descriptiva

Guión/instrucciones

- El curso busca que quienes participen en él adquieran conocimientos básicos de seguridad digital para integrar a las prácticas cotidianas de las ONGs y organizaciones de derechos humanos que les permita fortalecer su capacidad de resiliencia y sostenibilidad.
- Les recuerdo que en este módulo la aproximación a la seguridad digital se aborda desde una perspectiva de análisis de riesgo, y la idea concreta de esta tercera sesión es la de pensar en la seguridad digital desde la perspectiva de las comunicaciones internas y externas.
- En esta tercera sesión las personas que participan en el curso recibirán los elementos para desarrollar en su organización un plan básico que les permita mejorar prácticas cotidianas y con ello mejorar la seguridad digital de las mencionadas organizaciones.

Minuto 4	**Actividad/Acción de la persona facilitadora**	**Estrategia/Metodología**
	Introducción al tema	Relato sobre una visual descriptiva

Guión/instrucciones

- Durante esta tercera y última sesión reflexionaremos sobre qué sabemos de nuestras propias vulnerabilidades y capacidades de respuesta a esas vulnerabilidades. Recibiremos los elementos básicos para desarrollar un plan de respuesta a incidentes cibernéticos, una tarea que sus organizaciones deberán continuar después de esta sesión.
- Finalmente, recorreremos los 10 pasos básicos de una ruta de mejora de la seguridad digital para sus organizaciones.

Minuto 6	**Actividad/Acción de la persona facilitadora**	**Estrategia/Metodología**
	Introducción al primer tema de esta sesión	Relato sobre una visual descriptiva

Guión/instrucciones

- Lo primero que haremos será repasar conceptos claves de la seguridad digital en la perspectiva del análisis de riesgo.

Minuto 7	**Actividad/Acción de la persona facilitadora**	**Estrategia/Metodología**
	Recordar el balance en temas de seguridad digital	Relato sobre una visual informativa

Guión/instrucciones

- Para encontrar el equilibrio en materia de seguridad digital debemos identificar nuestros riesgos, los posibles ataques y las vulnerabilidades, esto es lo que nos permita establecer las buenas prácticas que se pueden implementar en las organizaciones.

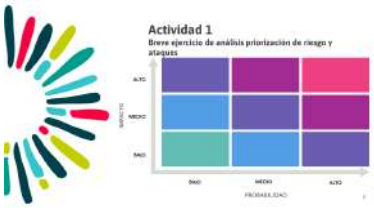
Minuto 8	**Actividad/Acción de la persona facilitadora**	**Estrategia/Metodología**
	Revisar los temas de Riesgos, ataques y vulnerabilidades	Relato sobre una visual descriptiva que contiene el texto a repetir.

		La diapositiva describe cuatro momentos importantes del ciclo de vida de la información. Quien facilita debe hacer énfasis en cada uno de estos pasos y diferenciarlos.

Guión/instrucciones

- *Leer la diapositiva.*
- Hemos hablado insistentemente sobre los riesgos, los posibles ataques y las más frecuentes vulnerabilidades que ustedes pueden sufrir. En esta oportunidad vamos a distribuirnos en grupos de 5 o 6 personas por grupo para durante 10 minutos para que cada grupo intercambie sus experiencias y determine de los riesgos y ataques cuales son los que más han sufrido o temen sufrir. Esto nos servirá para la actividad 3 de esta sesión. Cada grupo debe seleccionar los 4 riesgos y 4 ataques que consideran más importantes en su actividad.

REQUERIMIENTO DE LA PLATAFORMA: La personas facilitadora deberá habilitar los grupos y medir el tiempo para que cada grupo realice la actividad

Minuto 20	**Actividad/Acción de la persona facilitadora**	**Estrategia/Metodología**
	Actividad	Relato sobre una visual para desarrollar la actividad.

Guión/instrucciones

- Considerando los cuatro riesgos y ataques vulnerabilidades que se identificaron en cada grupo como más importantes en su actividad, ahora haremos un ejercicio grupal.
- La idea es que ahora reflexionen sobre qué tan probable es que suceda y cuál sería el impacto para su trabajo de cada una de esos cuatro ataques o riesgos que identificaron. Así por ejemplo si identificaron que la pérdida de información es un riesgo real en su organización, defina cuál es la probabilidad de suceda (si es alta, media o baja) y su impacto en la organización (alto, medio o bajo). Mientras diligencia el cuadro tendrá que ir decidiendo esto respecto de los demás que tiene en su lista pues al final solo debe haber un ataque o riesgo por cuadro, es una forma de priorizar y que el cuadro al final quede como un mapa de calor. Esto permitirá definir la prioridad para atender los principales riesgos y ataques.
- Si quieren, tengan presente que en la actividad que hicieron con su grupo eligieron nueve riesgos y ataques más importantes en sus organizaciones, el cuadro ofrece nueve espacios, ahora tienen la oportunidad de hacer los ajustes para su propia organización y agregar una novena, pero no es necesario. Lleguen hasta donde puedan, no tienen que hacer un ejercicio perfecto, piensen en esta actividad como una primera reflexión que podrán seguir trabajando después de este curso.
- Les doy cinco minutos para hacer el ejercicio. Empezamos
- *La persona facilitadora dará los cinco minutos para que se realice el ejercicio*
- Bueno, ya se cumplieron los cinco minutos, lo que pueden ver en el cuadro que cada persona realizó es una primera versión del análisis de riesgo de su organización. En rojo ven el riesgo o vulnerabilidad que para su organización es más prioritario de atender, seguido de los que queden en el color vino tinto, luego los que quedan en morado, azul y finalmente verde. Este ejercicio preliminar les servirá para discutir en sus organizaciones y acordar cuál es el cuadro final con el que trabajarán.
- *Abra el micrófono por un par de minutos para escuchar a las personas y lo que opinan del ejercicio*

Minuto 30	**Actividad/Acción de la persona facilitadora**	**Estrategia/Metodología**

	Revisar los temas de buenas prácticas	Relato sobre una visual descriptiva que recuerda información ya suministrada.

Guión/instrucciones

- Como vimos la sesión pasada, los riesgos más frecuentes para las Organizaciones No Gubernamentales y las de Derechos Humanos suceden porque se presentan también ataques frecuentes que aprovechan una serie de vulnerabilidades que están presentes en el entorno digital. La forma de mitigar esto es adoptando buenas prácticas, recuerden esto. Usen esta diapositiva para seguir el ejercicio

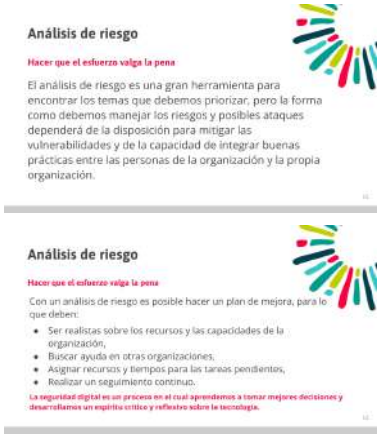
Minuto 32	**Actividad/Acción de la persona facilitadora**	**Estrategia/Metodología**
	Actividad	Relato sobre una visual para desarrollar la actividad.

Guión/instrucciones

- Tome el riesgo o ataque que en su cuadro quedó en rojo. Complete este cuadro para ese riesgo o ataque, identificando las vulnerabilidades que favorecen que ocurra y las buenas prácticas que lo evitan. De nuevo es volver a la idea de la balanza y buscar la forma de equilibrar. Posteriormente deberá repetir este ejercicio para cada uno de los riesgos y ataques que identificó.
- Tomen cinco minutos para iniciar colectivamente el ejercicio con el riesgo o ataque que han priorizado
- *De los cinco minutos para que las personas hablen del proceso*
- ¿Cómo les fue?
- *Abra el micrófono por un par de minutos para escuchar a las personas y lo que opinan del ejercicio*
- Antes de continuar quiero resaltar que lo importante es que las organizaciones identifiquen las formas que existen de mitigar los ataques o de prevenir los riesgos. Como no podremos completar el ejercicio esta vez, la idea es que se animen a seguir y entender que cuando hagan el ejercicio completo tendrán la información para enfrentar esos riesgos y ataques.

SUGERENCIA: La persona facilitadora debe poner entusiasmo en esta explicación, después de un módulo que aplasta un poco el ánimo debe quedar la sensación de que sí es posible hacer algo.

Minuto 42	**Actividad/Acción de la persona facilitadora**	**Estrategia/Metodología**
	Pasamos al segundo tema de contenido de la sesión 2	Introducción al tema sobre una visual general

Guión/instrucciones

- Como cierre de este punto hagamos unas reflexiones finales
- *leer las diapositivas de conclusión*

Minuto 45-55 DESCANSO	**Actividad/Acción de la persona facilitadora** Descansar	**Estrategia/Metodología** Parar durante 10 minutos

Guión/instrucciones

Minuto 55 	**Actividad/Acción de la persona facilitadora** Pasamos al segundo tema	**Estrategia/Metodología** Relato sobre una visual descriptiva

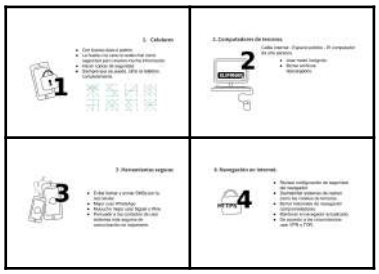
Guión/instrucciones

- Además de que el análisis de riesgo permite que su organización tenga ya una ruta para abordar los riesgos y ataques que se han priorizado, queremos dejarles también una ruta que puede servir a cualquier organización no gubernamental y a las que defienden derechos humanos, veamos.

Minuto 56 	**Actividad/Acción de la persona facilitadora** Explicar la ruta para una mejora básica de la seguridad digital de las organizaciones	**Estrategia/Metodología** Relato sobre una visual informativa

Guión/instrucciones

- Con base en lo que sabemos de los riesgos, ataques y vulnerabilidades más frecuentes entre las ONG y organizaciones de DDHH sabemos que la mejor forma de mejorar la seguridad digital este sería un plan de mejora para nuestra organización que nos permitiría reflexionar en cada paso y tomar decisiones, a veces son cambios internos (en lo que las siguientes diapositivas te pueden ayudar), otras veces es desarrollar políticas y en otras puede significar identificar quién nos puede ayudar.
- *La persona que facilita leerá cada uno de los 10 pasos*

Minuto 59	**Actividad/Acción de la persona facilitadora**	**Estrategia/Metodología**
  	Continuar explicando el concepto	Relato sobre una visual de infografía

Guión/instrucciones

- Finalmente, vamos a detenernos un poco en 10 recomendaciones importantes para mejorar nuestra seguridad digital, estos son cambios que podemos hacer en nuestro uso cotidiano de la tecnología y que debemos incentivar en toda la organización, parte del proceso de hacer el camino que vimos antes es reflexionar sobre cuáles de estas recomendaciones debemos integrar en cada paso, eso deberán hacerlo ustedes en sus organizaciones más adelante. Empecemos
- *(Pasando diapositiva por diapositiva la persona que facilita la sesión se detendrá en cada una).*
- Recomendación 1. Las claves que usamos en los dispositivos son importantes y no se deben menospreciar pues son el primer elemento de nuestra seguridad digital, por eso debemos poner atención a las claves que los protegen, acá algunas ideas que pueden implementar en sus celulares para enfrentar los riesgos, evitar ataques y mitigar nuestras vulnerabilidades . *Leer la diapositiva*
- Recomendación 2. En la encuesta se estableció que varias de las personas participantes en este curso usan cafés internet, espacio público -recuerden el caso que vimos la sesión pasada sobre el wifi público en los aeropuertos- o el computador de otra persona para conectarse a la red. Los consejos y lineamientos sobre cómo protegernos en estas circunstancias son especialmente importantes para las organizaciones en donde esto sucede. *Leer la diapositiva*
- Recomendación 3. Durante el curso hablamos sobre la importancia de las comunicaciones cifradas y eso supone que seamos muy conscientes en nuestra cotidianidad de usar herramientas seguras. Les proponemos que adquieran las siguientes prácticas que les hará pensar siempre en cuáles son las herramientas seguras y preferidas. *Leer la diapositiva*
- Recomendación 4. El uso regular de internet en nuestras organizaciones y la información que revelamos sobre las personas y las organizaciones a través de la navegación nos debería llevar a evaluar mejor las herramientas que usamos en la navegación e incluso a pensar en cómo las configuramos. Recuerden el ejercicio que hicimos para configurar WhatsApp de forma más segura, pueden buscar tutoriales para sus navegadores y también hacer el ejercicio con estas herramientas. En todo caso, también es importante recordar que a veces las medidas de seguridad hacen más lenta la navegación y por tanto, en condiciones de mala conectividad hay precauciones que será mejor no adoptar. *Leer la diapositiva*

Minuto 68	**Actividad/Acción del Facilitador**	**Estrategia/Metodología**
	Continuar explicando las recomendaciones de la ruta	Relato sobre una visual de infografía

Guión/instrucciones

- Recomendación 5. Considerando que no hay seguridad digital 100% una forma de enfrentar los riesgos es mitigar sus efectos. Hacer copias de respaldo es una forma efectiva de mitigar los riesgos de pérdida de información. Eso sí las copias deben estar cifradas. Por eso es importante que analicemos la herramienta que usamos, que la configuremos y entendamos cómo queda protegida nuestra información. Vale la pena recordar en todo caso que hay personas que intencionalmente eligen solo tener comunicaciones efímeras y asegurarse de borrar pronto todos sus mensajes como una forma de protección, esto es también válido y usualmente es el resultado de una profunda reflexión. *Recomendación 5 Leer la diapositiva.*
- *(la siguiente diapositiva elabora más en esta recomendación)* Vale la pena detenernos un momento en esta recomendación pues existen diferentes formas de hacer copias de respaldo. Lo importante es que revisen cuál es más funcional para cada organización. Pueden usar sus propios dispositivos (USB o discos duros) o servicios en la nube de terceros como Google Drive, iCloud. En todo caso, para la información sensible deben tener el respaldo cifrado. Para esto pueden usar VeraCrypt.

Minuto 75	**Actividad/Acción del Facilitador**	**Estrategia/Metodología**
	Continuar explicando las recomendaciones de la ruta	Relato sobre una visual de infografía

Guión/instrucciones

- Recomendación 6. Debemos tener cuidado con la información que publicamos en internet porque ésta revela mucho sobre las personas, sobre sus círculos personales, laborales y también sobre las organizaciones en las que trabajan o las que representan. Le proponemos una serie de reflexiones para que las decisiones sobre la información de la organización sean intencionales: *Leer la diapositiva*
- Recomendación 7. Volvamos a hablar de las contraseñas, esta vez para las herramientas que usamos. En las encuestas varias personas afirmaron que repiten contraseñas y varias cuentan que mantienen los navegadores permanentemente abiertos. A estas alturas del curso seguramente ya tenemos claro que las buenas prácticas con las contraseñas son quizá el elemento más básico de nuestra seguridad digital. *Leer la diapositiva*

- Recomendación 8. Una de las tareas importantes que debería quedar a quienes participaron del curso es la de pensar en la información sensible que manejan en la organización, esto depende mucho del tipo de organización que es y los datos que conservan, si es una organización que trabaja en temas de violencia contra las mujeres deberá definir cómo se manejan los datos que tienen y cómo y con quién los comparten, algo similar sucede con organizaciones que trabajan con personas migrantes, por ejemplo. Pero toda organización debe analizar la información que tiene y definir su grado de sensibilidad, por ejemplo tienen muchos datos de las personas que trabajan para ustedes que si se filtran o son divulgadas por ustedes mismos pueden servir para fraudes, chantajes o incluso abusos y algunas formas de violencia de género o de otro tipo. Por eso les proponemos que se hagan unas preguntas y reflexionen sobre la información sensible que tienen, es así como podrán entender la importancia de adoptar medidas para protegerla. No hacerlo puede vulnerar la intimidad de otras personas y también puede poner en riesgo a la organización misma: *Leer las diapositivas.*
- Recomendación 9. En la encuesta establecimos que muchas de las organizaciones usan redes sociales para publicar información, siendo así, conviene a las personas que participan de este curso analizar la forma como usan estas redes, entender que hay medidas que se pueden tomar para que esta actividad sea segura: *Leer la diapositiva*
- Recomendación 10. Finalmente, si hacer copias de seguridad es una buena práctica, tener acciones de "ciber higiene", que incluye borrar información a veces, es también un importante elemento de la seguridad digital de sus organizaciones: *Leer la diapositiva.*

Hemos llegado al final de nuestro módulo sobre seguridad digital, quizá un mensaje final que podemos dejar es que la seguridad digital es altamente contextual. Los riesgos que enfrentamos, los posibles ataques, varias de las vulnerabilidades de las que podemos ser objeto así como las medidas que podemos adoptar para mitigar y evitar estas circunstancias, dependen en gran medida del lugar en que vivimos o trabajamos, de las personas a nuestro alrededor, de las condiciones de nuestra conectividad, de los equipos a los que tenemos acceso y una larga lista de etcétera, por tanto, es importante que entendamos que: "no hay seguridad completa" "no hay soluciones de una sola talla que le sirvan a todas las personas" y "nuestra seguridad personal depende de la del grupo". Gracias por habernos acompañado en este camino.