Image not found or type unknown

El ciclo de vida de los datos como forma de entender el riesgo [actividad de profundización]

Esta actividad de aprendizaje consiste en entender la evaluación de riesgos desde la perspectiva del ciclo de vida de los datos. Todos las personas activistas, grupos, colectivos, organizaciones y movimientos sociales manejan datos – desde la recopilación/creación/recolección de datos hasta la publicación de información basada en datos.

Introducción



Esta actividad de aprendizaje consiste en entender la evaluación de riesgos desde la perspectiva del ciclo de vida de los datos. Todos las personas activistas, grupos, colectivos, organizaciones y movimientos sociales manejan datos – desde la recopilación/creación/recolección de datos hasta la publicación de información basada en datos.

Existen dos enfoques principales sobre la mecánica de esta actividad:

- El **taller general** funciona como un taller general de seguridad digital donde participan tanto personas que provienen de grupos y organizaciones como las que hacen activismo de manera más individual.
- El **taller organizacional** está pensado para un grupo específico. El contexto de este tipo de talleres es que los diferentes integrantes se reúnen para realizar una evaluación de riesgos de sus prácticas y procesos organizacionales de tratamiento de datos.

Los objetivos de aprendizaje y los temas generales son los mismos para ambos enfoques, pero las metodologías y técnicas de facilitación se adaptan a los distintos formatos.

Objetivos de aprendizaje

Al terminar esta actividad, serán capaces de:

- Entender qué consideraciones sobre riesgos y seguridad tener en cada etapa del ciclo de vida de los datos.
- Aplicar marcos de evaluación de riesgos a su seguridad personal y/o organizacional.

¿A quién se dirige esta actividad?

Esta actividad está pensada para activistas individuales (en una evaluación general de riesgos o un taller de seguridad digital) y para grupos (una organización, red o colectivo) que está en proceso de evaluación de riesgos. Existen dos formatos y dos enfoques en relación a esta actividad, según se trate de un taller general o un taller dirigido a un grupo específico.

También se puede utilizar como actividad de diagnóstico a fin de definir en qué prácticas o herramientas enfocarse para el resto del taller de seguridad digital.

Tiempo necesario

Esto depende del número de participantes y el tamaño del grupo. En general, esta actividad dura cuatro horas como mínimo.

Recursos

- Hojas de papelógrafo
- Marcadores
- Proyector para presentar el ciclo de vida de los datos y la guía de preguntas, además de comentarios de participantes, si es necesario.

Mecánica

(Esto se aplica a un taller de evaluación general de riesgos o de seguridad digital, donde activistas de diferentes contextos se encuentran en una capacitación. Los objetivos de aprendizaje siguen siendo los mismos, pero algunas tácticas de capacitación y facilitación difieren de las que se usarían en un taller para un grupo más establecido de personas.)

Parte 1: ¿Qué publicas?

Pregunta al grupo: **¿Qué publicas como parte de tu trabajo como activista?**

El punto es empezar con la parte más obvia del ciclo de vida de los datos – datos procesados que se comparten como información. Pueden ser investigaciones, artículos, publicaciones en blogs, guías, libros, sitios web, publicaciones en redes sociales, etc.

Pueden compartir las respuestas en el grupo grande, como si fuera una asamblea o plenaria. Sugerimos la técnica ‘palomitas de maíz’ (popcorn) donde se dan respuestas rápidas y breves – como el maíz cuando explota en la cacerola.

Parte 2: Presentación del ciclo de vida de los datos y consideraciones de seguridad

El objetivo de la presentación es recordar que existe un ciclo de vida en el manejo de datos. Los puntos esenciales de la presentación se encuentran aquí (ver presentación sobre puntos claves sobre el ciclo de vida de los datos -datalife cycle-basics-presentation.odp- y también **Presentación**).

Parte 3: Tiempo de reflexión sobre los ciclos de vida de los datos personales

Pídeles que elijan un ejemplo específico de algo que hayan publicado (un artículo, una investigación, un libro, etc) y que formen grupos pequeños en base a la similitud de sus trabajos. Cada persona tendrá 15 minutos para rastrear el ciclo de vida de los datos de su ejemplo y reflexionar. Las preguntas guía para este tiempo de reflexión serán las consideraciones de la presentación.

Posteriormente, los grupos tendrán 45 minutos para compartir cada quien sus respuestas y debatir.

Parte 4: Comentarios y consideraciones de seguridad

En lugar de pedir que cada grupo presente sus conclusiones, se planteará a cada grupo las preguntas que surgieron de la discusión en los subgrupos.

Estas son algunas preguntas que puedes utilizar para trabajar sobre el tiempo de reflexión y el debate en grupo:

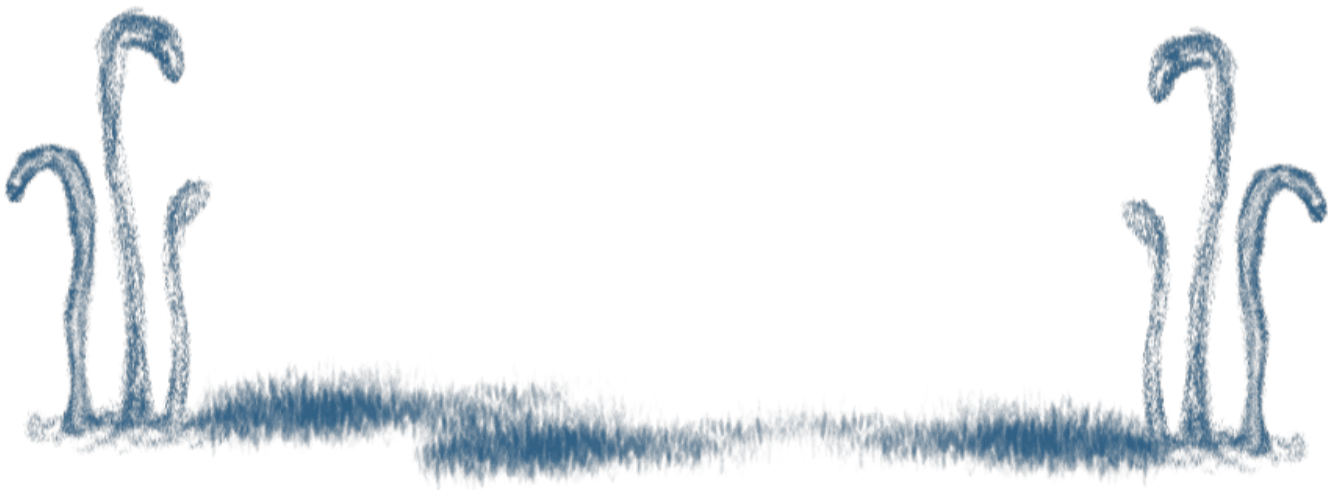
- ¿Cuáles son los dispositivos de almacenamiento de datos más comunes en tu grupo? ¿Cuáles fueron los que sólo una persona utiliza?

- ¿Cuáles fueron las diferencias y los puntos comunes en el acceso al almacenamiento de datos de tu grupo?
- ¿Qué pasa con el procesamiento de datos? ¿Qué herramientas se usaron en tu grupo?
- ¿Alguien del grupo publicó algo que le puso en riesgo directamente o a alguna persona conocida? ¿Qué fue lo que publicó?
- ¿Alguien del grupo había pensado en las prácticas de archivo y eliminación antes de hoy? Si es así, ¿qué prácticas utiliza?
- ¿Hubo algún interés en la seguridad en alguna parte del ciclo de vida de tus datos? ¿Qué tipo de interés/inquietud?

Síntesis de la actividad

Al final de las presentaciones e intercambios de los grupos, sintetiza la actividad de las siguientes maneras:

- Señala los puntos esenciales que se han detectado.
- Pide a las personas participantes señalar cuáles fueron los principales conocimientos adquiridos a través de la actividad.
- Pregúntales qué aprendieron durante la actividad en relación a los cambios que deberían introducir en su práctica de manejo de datos.



Mecánica para un taller organizacional

Pensado para un taller dirigido a una organización o grupo y sus integrantes.

Parte 1: ¿Qué tipo de información comparte cada unidad/programa/equipo/comité de la organización o grupo?

Según la configuración y la estructura de la organización o el grupo, pídele a cada equipo, área, comité o departamento que den un ejemplo de algo de lo que comparten – dentro o fuera de la organización o grupo.

Algunos ejemplos para promover una mayor respuesta:

- Para el área de comunicación – ¿qué informes publican?
- Para los equipos de investigación– ¿sobre qué investigación tienen que informar?
- Para los equipos administrativos y/o de finanzas – ¿quién tiene acceso a la planilla de sueldos de tu organización? ¿Y a los informes financieros?
- Para el departamento de recursos humanos – ¿Quién tiene acceso a las evaluaciones del personal?

Nota para la facilitación: Esta pregunta es mucho más fácil de contestar para los equipos que tienen objetivos de proyección exterior, por ejemplo, la sección de comunicación, o un programa que publica informes e investigaciones. Para las secciones de proyección más interna, como los sectores de finanzas, administración, o recursos humanos, posiblemente haya que dedicar más tiempo en la búsqueda de ejemplos de la información que comparten.

El objetivo, en esta etapa, es que cada equipo se dé cuenta de que en cualquier área se comparte información – dentro o fuera de la organización o grupo. Esto es importante porque cada equipo tiene que ser capaz de identificar uno o dos tipos de información que comparte al evaluar riesgos en su práctica de gestión de datos.

Parte 2: Presentación sobre el ciclo de vida de los datos y consideraciones de seguridad

La presentación consiste en recordar que existe un ciclo de manejo de datos. Los puntos claves de la presentación se encuentran aquí (ver la presentación sobre los puntos básicos del ciclo de vida de los datos - datalife cycle-basics-presentation.odp- y también **Presentación**).

Parte 3: Trabajo en grupos

Cada grupo tiene que identificar uno o dos tipos de la información que comparte/publica.

Con el fin de establecer prioridades, puedes sugerir que cada equipo piense en el tipo de información que le parece más importante cuidar, o qué clase de información delicada comparte.

Luego, deberán rastrear y analizar el ciclo de vida de los datos de cada uno de los tipos de información compartida o publicada. Utiliza la presentación siguiente para plantear las preguntas clave sobre la práctica de gestión de los datos que se aplica a cada pieza de datos publicada o compartida.

Al final de este proceso, cada equipo debería ser capaz de compartir el resultado de sus debates con todas las demás personas.

En general, el trabajo en grupos durará alrededor de una hora.

Parte 4: Presentaciones en grupo y reflexión sobre la seguridad

Según el tamaño de la organización o grupo y el trabajo que haya realizado cada unidad, dales tiempo para presentar las conclusiones de sus debates a sus colegas. Alienta a cada equipo a elaborar una presentación creativa y mostrar lo más destacable de sus conversaciones. No es necesario que compartan todo lo que conversaron.

Alienta a las demás personas que escuchen y tomen notas, ya que tendrán tiempo para compartir opiniones y comentarios al terminar cada presentación.

Se recomienda 10 minutos para cada grupo.

Quien facilita brinda sus comentarios al final de cada presentación, además de procurar que se respeten los tiempos y procesar los comentarios.

Algunas áreas sobre las que podrías hacer preguntas:

- Si se supone que el proceso de recolección de datos es privado, ¿no sería mejor usar herramientas de comunicación más seguras?
- ¿Quién tiene acceso al dispositivo de almacenamiento en teoría y en la realidad? En el caso de los dispositivos físicos de almacenamiento, ¿en qué parte de la oficina se encuentran?
- ¿Quién tiene acceso a los datos en bruto?

También puedes aprovechar la oportunidad para compartir algunas recomendaciones y sugerencias de prácticas más seguras de manejo de datos.

> **Nota para la facilitación:** Existe un recurso llamado Herramientas alternativas para vincular y comunicar que puede ayudarte a organizar esta actividad.

Parte 5: De vuelta a los grupos: Mejorar la seguridad

Una vez que todos los grupos hayan hecho su presentación, vuelvan a reunirse para seguir debatiendo y reflexionando cómo asegurar mejor sus datos y los procesos de gestión de los mismos.

El objetivo es que cada grupo planifique formas de operar con más seguridad en todas las etapas del ciclo de vida de los datos.

Al terminar el debate, cada equipo debe tener planes para que sus prácticas de gestión de datos se vuelvan más seguras.

> **Nota:** Partimos aquí de la suposición de que el grupo ya ha recibido una capacitación básica en seguridad para poder hacer esto. De lo contrario, quien facilita puede usar la Parte 4 para brindar algunas sugerencias de herramientas, opciones y procesos alternativos más seguros para las prácticas de almacenamiento de datos del grupo.

Preguntas guía para el debate en grupos

- De los tipos de datos que administras, ¿cuáles son públicos (cualquiera puede conocerlos), privados (sólo la organización o grupo puede conocerlos) o confidenciales (sólo el equipo y algunos grupos específicos de la organización pueden conocerlos)? ¿Y qué puede hacer tu equipo para garantizar que estos diferentes tipos de datos sean privados y confidenciales?
- ¿Qué puede hacer tu equipo para que puedas gestionar quién tiene acceso a tus datos?
- ¿Cuáles son las políticas de retención y eliminación de las plataformas que utilizan para almacenar y procesar sus datos en línea?
- ¿Cómo podría tener prácticas de comunicación más seguras el equipo, sobre todo en relación a la información y los datos privados y confidenciales?
- ¿Qué prácticas y procesos debería poner en práctica el equipo para preservar la privacidad y confidencialidad de sus datos?
- ¿Qué debería cambiar en su práctica de manejo de datos para volverla más segura? Observa los resultados del trabajo en grupo anterior y fíjate qué se puede mejorar.
- ¿Cuál sería el rol que debería tener cada uno de las integrantes del equipo para gestionar estos cambios?

Parte 6: Presentación final de los planes

Cada equipo tendrá un tiempo determinado para presentar cómo propone lograr que su práctica de gestión de datos sea segura.

Se trata de una buena oportunidad para que todos las personas dentro de la organización o grupo compartan estrategias y tácticas, y aprendan de las demás.

Síntesis de la actividad

Al final de las presentaciones y el intercambio entre los grupos, sintetiza la actividad de la forma siguiente:

- Señala los puntos claves que se plantearon;
- Pregunta cuáles son los principales conocimientos adquiridos en esta actividad;
- Llega a un acuerdo sobre los pasos siguientes para poner en marcha los planes.

Presentación

Otra forma de entender los riesgos es observar la práctica de tratamiento de datos de una organización o grupo. Todas trabajan con datos y cada una de las áreas o divisiones internas también.

Así, existen algunas consideraciones a tener para cada etapa del ciclo de vida de los datos.

Creación/recopilación/recolección de datos

- ¿Qué tipo de datos se están recopilando?
- ¿Quién crea/recopila/recolecta datos?
- ¿Acaso eso pone en riesgo a las personas? ¿Quién está en riesgo por la publicación de esos datos?
- ¿Qué tan público/privado/confidencial es el proceso de recopilación de datos?
- ¿Qué herramientas se utilizan para garantizar la seguridad del proceso de recopilación de datos?

Almacenamiento de datos

- ¿Dónde se almacenan los datos?

- ¿Quién tiene acceso al almacenamiento de datos?
- ¿Qué prácticas/procesos/herramientas utilizan para garantizar la seguridad del dispositivo de almacenamiento?
- Almacenamiento en la nube vs. almacenamiento físico vs almacenamiento en dispositivos.

Procesamiento de datos

- ¿Quién procesa los datos?
- ¿El análisis de los datos puede poner en riesgo a algún individuo, o al grupo?
- ¿Qué herramientas se utilizan para analizar los datos?
- ¿Quién tiene acceso al sistema/proceso de análisis de datos?
- En el procesamiento de datos, ¿se guardan copias secundarias de los datos en algún sitio?

Publicación/intercambio de información obtenida al procesar los datos

- ¿Dónde se publica la información/conocimiento?
- ¿La publicación de la información pone a alguien en riesgo?
- ¿Cuál es el público objetivo de la información publicada?
- ¿Tienes control sobre cómo se publica la información?

Archivo

- ¿Dónde se archivan los datos y la información procesada?
- ¿Los datos brutos se archivan, o sólo se archiva la información procesada?
- ¿Quién tiene acceso al archivo?
- ¿Cuáles son las condiciones de acceso al archivo?

Eliminación

- ¿Cuándo se eliminan de manera permanente (purgan) los datos?

- ¿Cuáles son las condiciones de eliminación?
- ¿Cómo podemos asegurarnos de que se eliminan todas las copias?

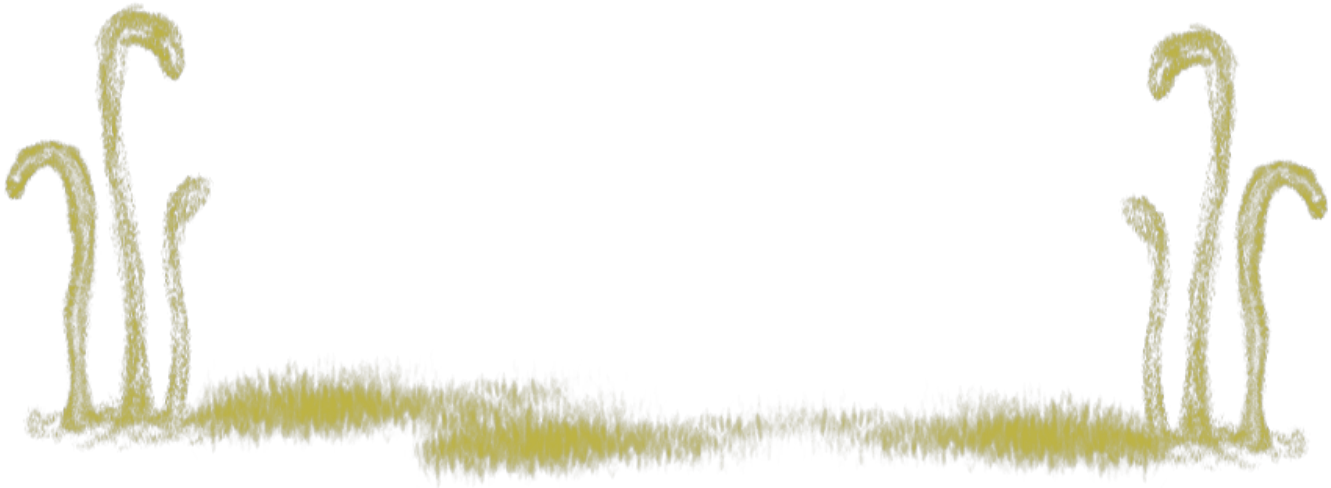
Notas para la facilitación

- Esta actividad sirve para poder conocer y evaluar los contextos, prácticas y procesos de seguridad de datos de quienes participan en este taller. Es mejor enfocarse en ese aspecto en lugar de esperar que esta actividad genere estrategias y tácticas para aumentar la seguridad digital.
- En un taller organizacional, puede ser mejor tener en cuenta los recursos humanos y los equipos/unidades administrativos. Para las nuevas personas integrantes de los grupos y organizaciones, muchas veces no cuentan con experiencia previa en talleres de seguridad digital y todos estos temas resultan muy nuevos para ellas. Por otro lado, es más difícil darse cuenta del hecho que el trabajo interno también implica “publicar datos”: datos delicados como la información sobre el equipo de trabajadores, salarios, notas sobre las reuniones del directorio, detalles bancarios de la organización, etc.
- Préstale atención también a los dispositivos físicos de almacenamiento. Si existen archivadores o armarios dónde se almacenan copias impresas de documentos, pregunta dónde están y quién tiene acceso a ellos. A veces, existe la tendencia a enfocarse demasiado en el almacenamiento en línea, olvidando así crear tácticas más seguras para el almacenamiento físico.

Lecturas recomendadas (optativo)

- Herramientas alternativas para vincular y comunicar (FTX: Reboot de seguridad)
- Seguridad móvil (FTX: Reboot de seguridad)
- Electronic Frontier Foundation's Surveillance Self-Defense (Defensa propia ante la vigilancia, de la Fundación Electronic Frontier, sólo en inglés) – a pesar de dirigirse sobre todo a un público estadounidense, esta guía contiene secciones muy útiles que explican los conceptos de vigilancia y las herramientas que se pueden usar para burlar los intentos de vigilancia.

- Guía de herramientas seguras de chat grupal y conferencias de Front Line Defenders (sólo en inglés) – una guía de gran utilidad sobre varios servicios y herramientas de chat y conferencia que cumplen con los criterios de seguridad de Front Line Defenders en relación a una aplicación o un servicio.
- Sitio web Privacy Not Included de Mozilla Foundation – analiza las diferentes políticas y prácticas de privacidad y seguridad de diversos servicios, plataformas y dispositivos para ver si cumplen con las Normas mínimas de seguridad de Mozilla, que incluyen cifrado, actualizaciones de seguridad y políticas de privacidad.



Revision #5
Created 26 April 2023 00:39:50 by Kira
Updated 28 July 2023 15:03:52 by Kira