Image not found or type unknown

Elementos básicos en la evaluación de riesgos [material de base]

Introducción

Todo el tiempo estamos evaluando riesgos. Así es como sobrevivimos. No se trata de un proceso que realizamos exclusivamente en el ámbito de la seguridad digital y/o informática.

Cuando salimos a caminar de noche por una calle tranquila, decidimos por qué acera vamos a caminar, cómo comportarnos, qué preparar y cómo caminar según nuestra lectura de la situación: *¿Esta calle es conocida por ser peligrosa? ¿Conozco a alguien en esta calle que podría venir en mi ayuda? ¿Puedo correr a toda velocidad si algo sucede? ¿Llevo pertenencias de valor con las que podría negociar? ¿Llevo objetos conmigo que podrían ponerme en peligro? ¿De qué lado de la calle es mejor caminar para evitar posibles riesgos?*

Cuando nuestro grupo empieza a planificar un nuevo proyecto, solemos pensar también en los posibles fracasos. Tomamos decisiones basándonos en lo que sabemos sobre el contexto y los factores que podrían hacer que no se cumplan los objetivos.

Al organizar manifestaciones y protestas, buscamos la forma de mantener a salvo tanto a quienes participan en la acción, como a la acción misma. Organizamos sistemas de compañerismo. Nos aseguramos de que haya un apoyo legal inmediato en caso de arrestos. Enseñamos, a quienes participan, conductas que puedan evitar abusos por parte de las autoridades y pensamos estrategias para realizar la protesta de manera pacífica a fin de minimizar potenciales riesgos.

También incluimos gente dedicada específicamente a mantener la seguridad de la acción.

Si bien la evaluación del riesgo puede ser algo que hacemos instintivamente, se trata de un proceso específico que llevamos a cabo – generalmente de manera colectiva – a fin de saber cómo evitar amenazas y/o responder a dichas amenazas.

Evaluación de riesgo: Dentro y fuera de la red

Evaluar los riesgos que corremos en línea no es algo tan instintivo, por diversas razones. La mayoría ni entiende cómo funciona internet ni cuáles son los riesgos y amenazas que implica– una realidad en constante cambio y crecimiento. Hay quienes tienen la sensación de que las actividades, acciones y comportamientos en línea no son “reales” y tienen efectos menos graves que lo que nos sucede físicamente. En el otro extremo del espectro, quienes ya tuvieron la experiencia de ver cómo la vida “real” de una persona se ve afectada por sus actividades en línea (personas que fueron engañadas en los sitios de citas, gente cuyas interacciones tabúes en internet se volvieron públicas, activistas arrestadas por decir algo contra el gobierno) tienden a tener una visión paranoica de internet.

La realidad es que, para muchas personas activistas, la oposición entre el fuera y dentro de la red es falsa. El uso de dispositivos digitales (teléfonos móviles, laptops, tabletas, computadores, etc),servicios, aplicaciones y plataformas basadas en internet (Google, Facebook, Viber, Instagram, WhatsApp, etc.) es algo común y básico en su trabajo – tanto para organizarse, como para el activismo en sí mismo. El modo en que nos organizamos y realizamos nuestra labor como activistas ha evolucionado a medida que la tecnología ha ido avanzando y desarrollándose – y seguirá siendo así. Internet y las tecnologías digitales son una de las claves de nuestra infraestructura organizativa. Las utilizamos para comunicarnos, coordinar y realizar actividades y construir nuestra comunidad. Las reuniones y eventos presenciales suelen desarrollarse junto con una participación en línea, sobre todo en las redes sociales y mediante hashtags (etiquetas). Actualmente, en muchas protestas, hay un constante flujo entre la movilización, la organización y las reuniones en línea y fuera de línea.

En lugar de considerar que lo que sucede en internet es algo separado de nuestra realidad física, piensa en las realidades en línea <-> fuera de línea como planos interconectados y porosos,

permeables. Existimos en ambas dimensiones de la realidad, la mayor parte del tiempo, al mismo tiempo. Lo que sucede en una, afecta nuestro modo de estar en la

Esto significa también que los riesgos y las amenazas en línea afectan nuestra integridad física fuera de línea y viceversa. Por ejemplo, las estrategias avanzadas de vigilancia estatal contra activistas y movimientos sociales que explotan el uso inseguro de las tecnologías (por ejemplo, cliquear links o descargar y abrir archivos no verificados/desconocidos potencialmente inseguros) para conseguir más información que les permita seguir vigilando también fuera de internet. . Quienes hayan tenido experiencias de violencia de género en línea conocen los efectos psicosociales de ese tipo de ataques y acoso. Hasta hay casos donde llega a afectar la seguridad física de las personas a las que estaba dirigida. Existen diferentes formas (acoso, *doxing*, hostigamiento) y se utilizan como tácticas de censura y sumisión contra activistas feministas y queer.

Pensar en la naturaleza permeable de las amenazas y los riesgos en línea <-> fuera de línea puede ser abrumador – *¿dónde empezamos a evaluar y saber cuáles son las amenazas y de dónde vienen?¿cómo elaboramos estrategias para lidiar con ellas?*

¿Qué es la evaluación de riesgos?

La evaluación de riesgos es el *inicio del proceso* de volverse más resiliente a la hora de responder ante contextos y amenazas cambiantes. Tiene como objetivo poder elaborar tácticas y estrategias para mitigar tales riesgos, y también tomar decisiones más informadas.

En términos generales, el riesgo es la exposición a posibles daños, lesiones o pérdidas.

En la evaluación de riesgos, se trata de la capacidad (o falta de capacidad) de una persona o grupo para responder a los impactos de una amenaza que se vuelve real o para evitar que suceda en primer lugar.

Existe una fórmula conocida para la evaluación de riesgos:

Riesgo = amenaza x probabilidad x impacto/capacidad

Donde:

- Amenaza es cualquier acción negativa que apunte hacia una persona o un grupo.
    - Las amenazas directas son intenciones explícitas de causar daño.
    - Las amenazas indirectas son las que suceden como resultado de un cambio en una situación.
    - Al definir cuáles son las amenazas o peligros, es importante definir de dónde vienen. Mejor aún, saber de quién vienen.

- La probabilidad es la posibilidad de que una amenaza se vuelva real.
    - Un concepto relativo a la probabilidad es la vulnerabilidad. Puede ser que el lugar, la práctica y/o la conducta del individuo/grupo incrementen las oportunidades para que un riesgo se convierta en un hecho.
    - Se trata también de la capacidad de quienes amenazan, sobre todo en relación con el individuo/grupo amenazado.
    - Para evaluar la probabilidad, pregunta si hay ejemplos reales de una amenaza de ese tipo que se haya cumplido para una persona o un grupo que conozcas – y compara la situación con la que vives de primera mano.

- El impacto es lo que sucederá cuando la amenaza se cumpla. Las consecuencias de la amenaza.
    - El impacto puede afectar al individuo, al grupo, a la red, o al movimiento.
    - Cuanto mayor sea el grado y/o el número de impactos de un peligro, mayor será el riesgo.

- Las capacidades son las habilidades, fortalezas y recursos a los que un grupo tiene acceso a fin de minimizar la probabilidad de que se cumpla la amenaza, o de responder al impacto causado por la misma.

Casos de estudio - amenazas y mitigación

Estudio de caso: Deya

A modo de ilustración, vamos a utilizar la experiencia ficticia, aunque bastante común, de Deya. Deya es una activista feminista que utiliza su cuenta de Twitter para desafiar a quienes promueven la cultura de la violación. En consecuencia, Deya ha sido acosada y amenazada en línea.

La amenaza que más le preocupa es la de quienes prometieron descubrir dónde vive y compartir la información en internet para invitar a otras personas a causarle daños físicos. En este caso, el impacto es claro – daño físico. Hay otras amenazas, como el acoso en el ámbito laboral para que la despidan de su trabajo y hacia su círculo visible de amistades en línea.

Para evaluar los riesgos, Deya tendrá que repasar todas las amenazas y analizarlas a fin de evaluar su probabilidad y el impacto que pueden causar – con el objetivo de planear cómo mitigar dichos riesgos.

Amenaza 1: Se descubre dónde vive y se comparte la información en línea

La mayoría de las amenazas proceden de cuentas en línea – y la mayoría de estas cuentas son de personas que no conoce y no puede verificar si se trata de personas de verdad o cuentas falsas. Deya reconoce a algunas de las personas que participan en las amenazas en línea: son actores conocidos que suelen participar en ataques en línea contra mujeres. Basándose en el conocimiento que tiene de ataques previos en los que a veces se publicaron detalles personales en línea, Deya siente un temor verdadero en relación a su seguridad personal.

¿Hay alguna forma de evitar que eso suceda? ¿Cuál es la probabilidad de que las personas que la acosan y atacan averigüen dónde vive ? Deya tiene que imaginar qué tan probable es que su dirección ya se encuentre disponible en internet, o que alguno de sus atacantes la ponga a disposición.

Para evaluar esta situación, Deya puede empezar realizando una búsqueda en internet sobre sí misma para ver qué información encuentra – de esta manera, sabrá si hay espacios físicos asociados a su persona y si esos espacios señalan su verdadera localización física. Si descubre que su dirección se puede encontrar en internet, ¿qué puede hacer para evitar que esté disponible públicamente?

Deya también puede evaluar qué tan vulnerable o seguro es su domicilio. *¿Vive en un edificio con vigilancia y protocolos para el acceso de quienes no residen allí? ¿Vive en un apartamento que debe cuidar por su cuenta? ¿Vive sola? ¿Cuáles son las vulnerabilidades de su domicilio?*

Además, tendrá que evaluar cuáles son las capacidades y recursos que tiene para protegerse. *Si su domicilio se da a conocer públicamente en internet ¿puede mudarse? ¿Quién puede ofrecerle apoyo durante ese tiempo? ¿Puede llamar a las autoridades para pedir protección?*

Amenaza 2: Acoso en el ámbito laboral para que despidan a Deya de su trabajo

Deya trabaja en una ONG de derechos humanos, de modo que no hay peligro de que la despidan de su empleo. Pero el domicilio donde se encuentran las oficinas de la organización es públicamente conocido en su ciudad y está disponible en el sitio web de dicha organización.

Para Deya, el peligro de perder su empleo es escaso. Sin embargo, la información públicamente disponible sobre su ONG puede ser un flanco vulnerable para su seguridad física, así como para la seguridad del equipo.

En este escenario, la organización deberá hacer su propia evaluación de riesgo, a raíz del hecho de que una de las integrantes del equipo de trabajo es blanco de amenazas.

¿Qué hacer con los riesgos? Tácticas generales de mitigación

Más allá de identificar y analizar amenazas, probabilidades, impactos y capacidades, la evaluación de riesgos tiene que ver también con la elaboración de un plan de mitigación para todos los riesgos identificados y analizados.

Hay cinco maneras generales de mitigar riesgos:

Aceptar el riesgo y elaborar planes de contingencia

Algunos riesgos son inevitables. O ciertos objetivos hacen que valga la pena correrlos. Pero eso no significa que haya que desestimar su importancia. Hacer un plan de contingencia significa

imaginar qué pasaría si sucediera el mayor riesgo y cuáles serían los impactos más graves para poder dar los pasos necesarios para lidiar con la situación.

Evitar el riesgo

Implica reducir la probabilidad de que una amenaza se vuelva un hecho. Puede significar la implementación de políticas de seguridad para mantener más seguro al grupo. También podría implicar cambios de comportamiento para incrementar las posibilidades de evitar un riesgo específico.

Controlar el riesgo

A veces, un grupo puede decidir enfocarse en el impacto causado por la amenaza, en lugar de centrarse en ella. Controlar el riesgo significa reducir la gravedad de su impacto.

Transferir el riesgo

Conseguir un recurso externo para asumir el riesgo y su impacto.

Monitorear el riesgo para estar alerta de cambios en términos de probabilidad e impacto

Suele emplearse esta táctica de mitigación para los riesgos de bajo nivel.

Estudio de caso: Deya

Para usar el ejemplo de Deya otra vez, ella tiene alternativas para actuar frente a los riesgos que enfrenta basándose en su análisis y evaluación, la probabilidad de que ocurran, los impactos y las capacidades que ya existen para lidiar con las amenazas y/o los impactos que puedan tener.

En el caso en que la dirección postal de Deya ya se pueda encontrar en internet, ella tiene que aceptar el riesgo y enfocarse en realizar planes de contingencia. Estos planes pueden ser desde mejorar la seguridad de su hogar, hasta mudarse. La medida de las posibilidades dependerá de las realidades y contextos existentes de Deya.

Otra opción que tendría Deya en este escenario sería preguntar dónde es que se encuentra su dirección postal disponible al público para eliminar ese contenido. Sin embargo, esta no es una táctica infalible. Le ayudará a eliminar el peligro si ninguna de las personas que la acosan vieron

todavía la información. Pero si alguna de esas personas ya lo ha hecho y tomó una fotografía o captura de pantalla de la información, es muy poco lo que puede hacer Deya para impedir que se divulguen los datos.

Si la dirección de donde vive Deya no se conoce públicamente y no está disponible en internet, hay más espacio para pensar en cómo evitar riesgos. ¿Qué puede hacer Deya entonces para impedir que las personas que la acosan descubran la dirección de su casa? Puede eliminar sus publicaciones con etiquetas geográficas que estén cerca de su casa y dejar de enviar posts en tiempo real que contengan esta información.

En cualquiera de los dos escenarios posibles (ya sea que su domicilio esté disponible públicamente o no), Deya puede dar los pasos necesarios para controlar el riesgo enfocándose en proteger su hogar.

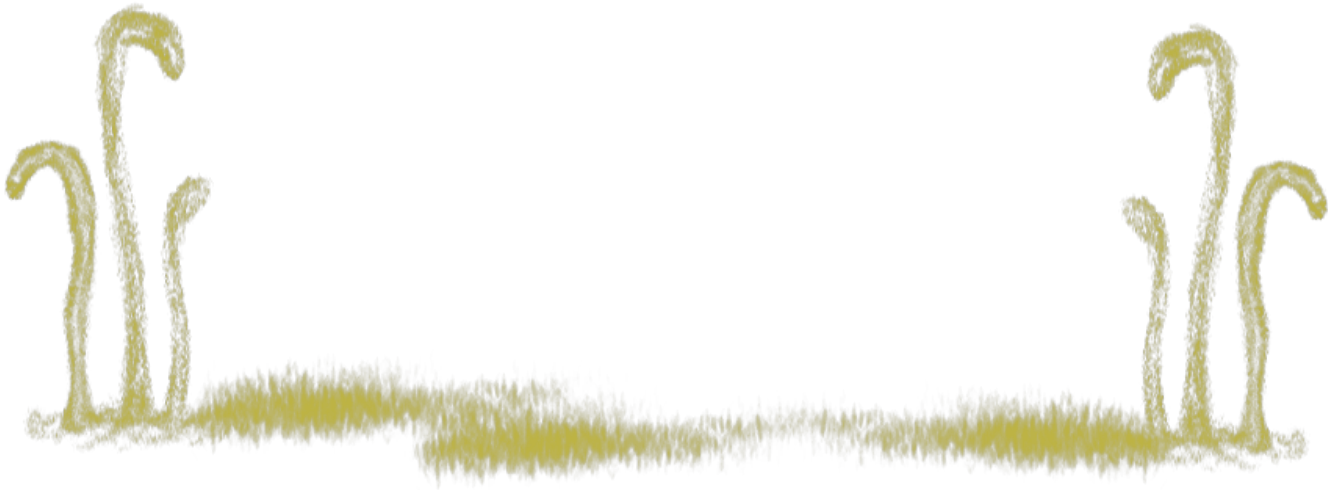
Las buenas estrategias de mitigación de riesgos implican pensar en estrategias preventivas y dar respuesta frente a incidentes – evaluar lo que se puede hacer para evitar el peligro y pensar qué se puede hacer si la amenaza se cumple.

Estrategias de prevención

- ¿Con qué capacidades cuentas para evitar que esta amenaza se vuelva un hecho?
- ¿Qué acciones llevarás a cabo para evitar que suceda? ¿Cómo cambiarás los procesos adentro de la red?
- ¿Tienes que crear políticas y procedimientos ?
- ¿Qué capacidades necesitas para prevenir esta amenaza?

Respuesta frente a incidentes

- ¿Qué harás cuando esta amenaza se torne realidad? ¿Qué pasos darás?
- ¿Cómo reducirás la gravedad del impacto de esta amenaza?
- ¿Qué capacidades se necesitan para dar los pasos necesarios para responder a esta amenaza?



Recordatorios

Las evaluaciones de riesgos están sujetas a plazos determinados

Es decir, se dan en un período de tiempo específico – en general, cuando surge una amenaza nueva (por ejemplo, un cambio de gobierno, cambios en las políticas de seguridad de alguna plataforma, etc), o se sabe de una nueva amenaza (por ejemplo, acoso en línea contra activistas, denuncia de cuentas de activistas comprometidas, etc), o se produce un cambio dentro de un colectivo (un nuevo proyecto, nuevo liderazgo). Por lo tanto, es importante revisar las evaluaciones de riesgo ya realizadas porque los riesgos van cambiando a medida que van surgiendo y desapareciendo amenazas, y a medida que van cambiando las capacidades de los grupos y las personas para responder ante una amenaza y recuperarse de sus impactos.

La evaluación de riesgos no es una ciencia exacta

Cada una de las personas que integran un grupo que está realizando un proceso de evaluación de riesgos tiene una perspectiva y una posición que afecta su capacidad de saber la probabilidad de que una amenaza se concrete, y también su capacidad de evitarla o responder a los impactos que causa. El objetivo de la evaluación de riesgos es entender colectivamente estas diferentes perspectivas adentro del grupo y llegar a tener una conciencia de los riesgos a los que se enfrenta. Las evaluaciones de riesgos son relativas. Diferentes grupos de personas enfrentados a los mismos riesgos y peligros tienen diferentes capacidades para evitarlos y/o responder ante las

consecuencias.

La evaluación de riesgos no garantiza 100% la seguridad, pero puede ayudar a un grupo a prepararse para enfrentar amenazas

Dado que no existe nada que sea 100% seguro y a salvo, las evaluaciones de riesgos no pueden garantizar total seguridad. Pero pueden ayudar a individuos y grupos a evaluar los riesgos y amenazas que pueden afectarlos.

La evaluación de riesgos tiene que ver con la capacidad de analizar riesgos conocidos y emergentes a fin de darse cuenta de cuáles son los riesgos que son impredecibles

Existen diferentes tipos de riesgos:

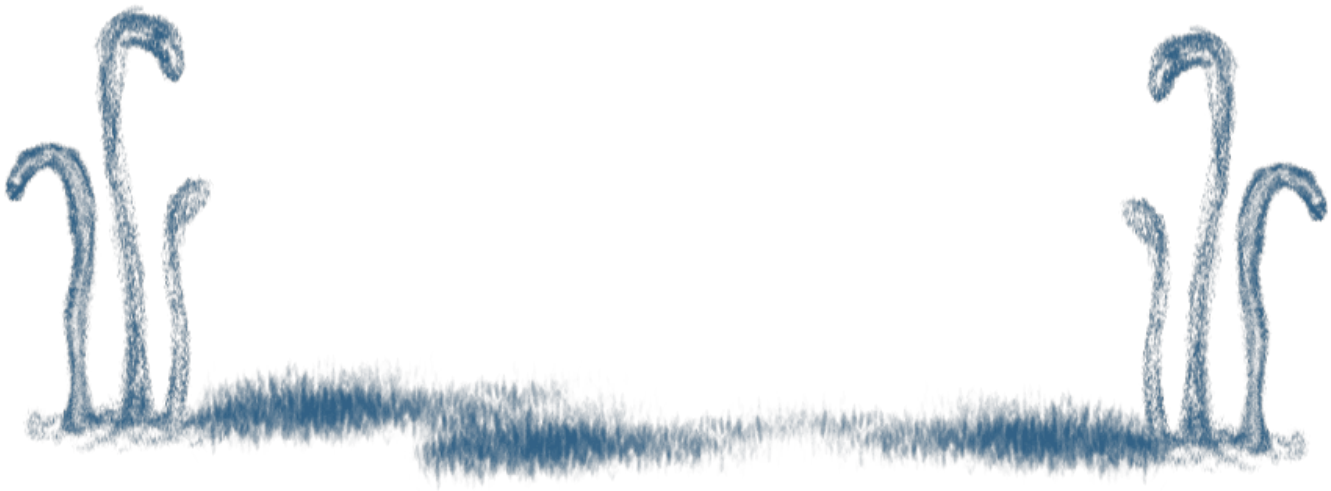
- Riesgos conocidos: peligros y amenazas que ya se han entendido en la comunidad. ¿Cuáles son sus causas? ¿Qué impactos tienen?
- Riesgos emergentes: amenazas que se han vuelto realidad pero no dentro de la comunidad a la que pertenece la persona. Pueden ser amenazas resultantes del clima político que se vive, de los desarrollos tecnológicos y/o cambios dentro de las comunidades de activistas en general.
- Riesgos desconocidos: son los riesgos imprevisibles, aquéllos cuya ocurrencia y momento de ocurrencia resulta imposible prever.

Las evaluaciones del riesgo son importantes para la planificación

Permiten que el individuo o el grupo analicen qué es lo que puede causarles daño, las consecuencias de tales daños y las capacidades con las que cuentan para mitigarlos . El desarrollo de un proceso de evaluación de riesgos ayuda a los grupos a tomar decisiones realistas sobre los riesgos que enfrentan y les permite prepararse.

La evaluación de riesgos es una forma de controlar el miedo y la ansiedad

Se trata de un buen proceso para conocerlos temores de las personas que integran un grupo – para generar equilibrio entre la paranoia y la total ausencia de miedo (pronoia) a fin de tomar decisiones colectivamente sobre qué riesgos tener en cuenta en la planificación.



Revision #3
Created 26 April 2023 00:40:41 by Kira
Updated 28 June 2023 18:49:16 by Kira