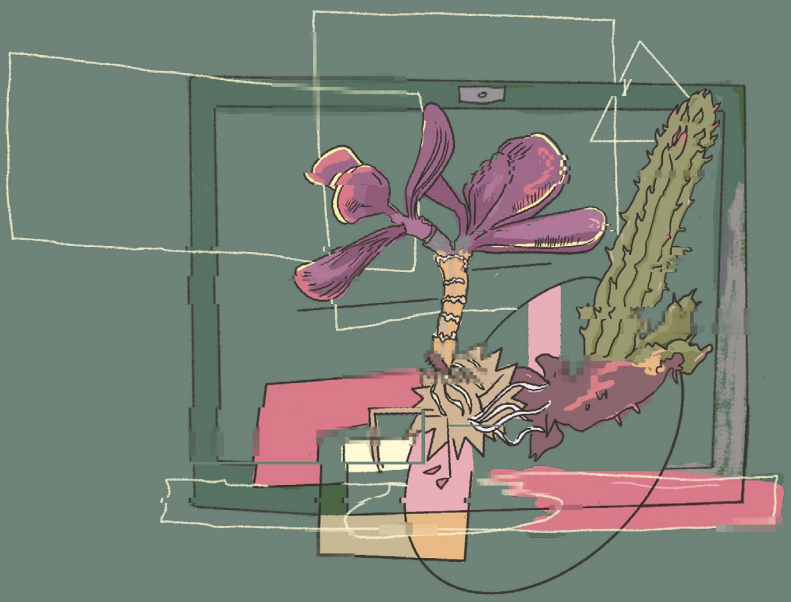
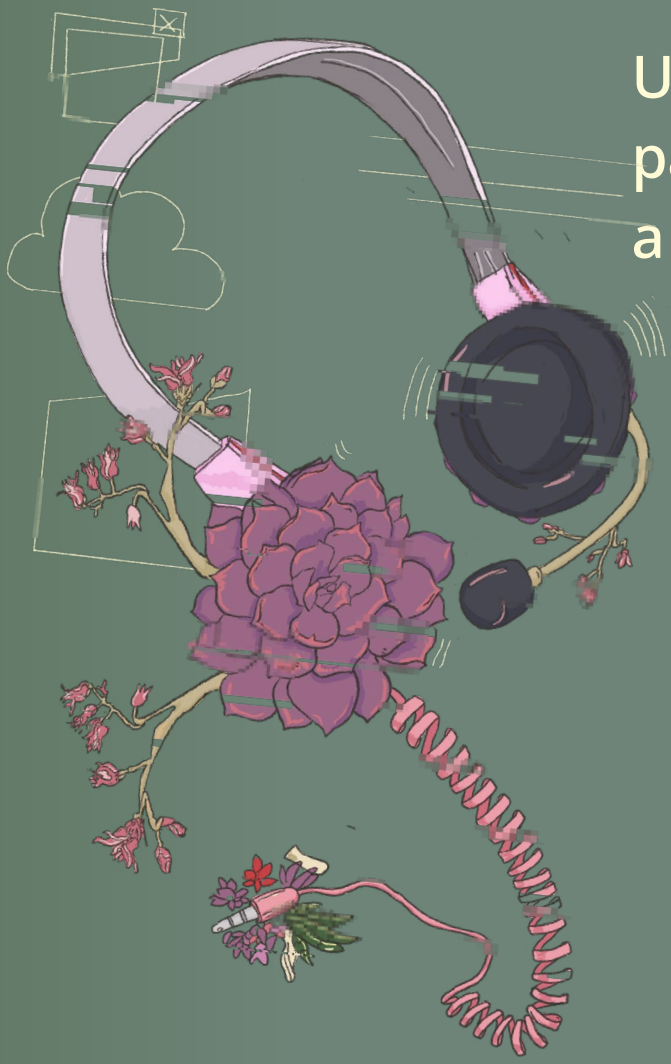


CuidaTech

Una guía paso a paso
para brindar apoyo digital
a la sociedad civil



Créditos

Coordinadora y coeditora:

Flo Pagano, Digital Defenders Partnership

Coeditora:

Inés Binder, Digital Defenders Partnership

Diseño y diagramación:

Constanza Figueroa

Traducción al español:

Zenobia Traducción

Contribuciones:

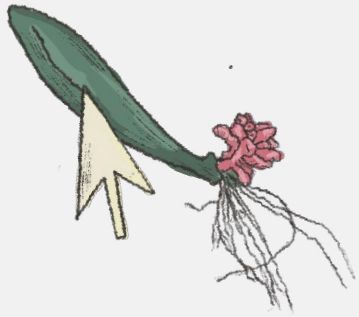
Daniel Bedoya Arroyo, Access Now Digital Security Helpline
Inés Binder, Digital Defenders Partnership
Jean-Marc Bourguignon, Nothing2Hide
Michel Carbone, Access Now Digital Security Helpline
Mohamed Chennoufi, Access Now Digital Security Helpline
Farhanah, Digital Defenders Partnership
Alexandra Haché, Digital Defenders Partnership
Maggie Haughey, Access Now Digital Security Helpline
Rogelio López, Access Now Digital Security Helpline
Beatrice Martini, Access Now Digital Security Helpline
Etienne Maynier, Amnesty Tech
Daniel Ó Cluanaigh, Digital Defenders Partnership
Lu Ortiz, Vita Activa
Flo Pagano, Digital Defenders Partnership
Grégoire Pouget, Nothing2Hide
Hassen Selmi, Access Now Digital Security Helpline

CuidaTech

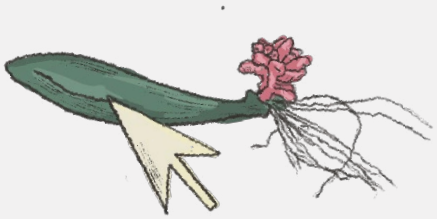
Una guía paso a paso para brindar apoyo digital a la sociedad civil

Índice de contenidos

Introducción

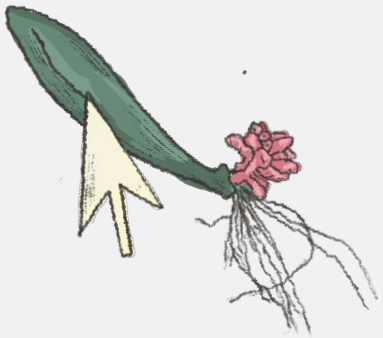


Las organizaciones que ofrecen apoyo a la sociedad civil en materia de seguridad digital se han multiplicado en la última década. Las personas defensoras de derechos humanos, activistas, periodistas, organizaciones LGTBQIA+ y otras minorías que sufren ataques constatan cómo las TIC se convierten en una herramienta crucial para sus actividades y, a su vez, en un arma poderosa para minar su labor, lo que puede suponer una amenaza tanto para ellas como para sus aliadas.



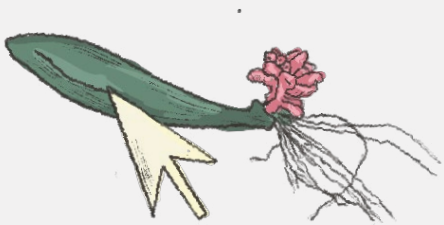
Han pasado diez años desde que, en la primera mitad de la década de 2010, algunos colectivos tecnológicos radicales empezaran a brindar apoyo técnico a activistas y organizaciones internacionales a través de proyectos que proporcionaban asesoramiento y formación en seguridad digital a grupos de la sociedad civil y a personas defensoras de los derechos humanos.

A lo largo de estos años dicho empeño se ha multiplicado. Organizaciones grandes y pequeñas, en todas las regiones del planeta, han creado líneas de atención sobre seguridad digital para las comunidades más diversas: periodistas y personas defensoras de derechos humanos, organizaciones internacionales y movimientos de base, grupos LGTBQIA+, centros de acogida para mujeres, etc.



En 2015 estas líneas de atención comenzaron a trabajar de forma más sistemática gracias a la creación de CiviCERT, una red de líneas de atención y proveedores de infraestructuras digitales para la sociedad civil. De las cinco organizaciones fundadoras, CiviCERT se ha expandido a más de treinta, entre las cuales hay organizaciones locales e internacionales, y personas que, a título individual, ofrecen asistencia en materia de seguridad digital en su país o región.

Además, en un contexto en el que los ataques digitales hacia la sociedad civil y las minorías vulnerables no paran de aumentar, tanto en cantidad como en intensidad, se están creando nuevas líneas de atención sobre seguridad digital en todo el mundo. Sin embargo, ya no están orientadas exclusivamente a movimientos sociales, sino también a brindar apoyo a mujeres, personas LGTBQIA+ y otros actores que son objeto de violencia y vigilancia focalizada a través de las TIC.



En este contexto, CiviCERT comenzó a recibir solicitudes para acompañar la creación de nuevas líneas de atención sin fines de lucro. En algunos casos, se aunaron esfuerzos para ofrecer orientación, formación e infraestructura a las líneas de atención recién creadas o por crearse. En otros casos, cuando únicamente se solicitaba una orientación inicial, se constató que la documentación existente era insuficiente. La mayoría había sido desarrollada para equipos

comerciales y gubernamentales de respuesta a incidentes de seguridad informática, que no están familiarizados con el contexto de la sociedad civil, o bien para líneas de atención humanitaria que no tienen experiencia en emergencias de seguridad digital.

Faltaba un conjunto de instrucciones sencillas que permitieran navegar por los flujos de trabajo y procedimientos de una línea de atención sobre seguridad digital centrada en las necesidades específicas de grupos que, a menudo, carecen de fondos y de personal, que no funcionan de forma jerárquica y cuyos equipos están expuestos a amenazas y al consiguiente riesgo de trastorno de estrés postraumático.

Con la publicación de esta guía queremos cubrir ese vacío de modo que las organizaciones más pequeñas y colectivos de base puedan conformar equipos que respondan a las necesidades de seguridad digital de las personas con quienes trabajan y luchan de manera cotidiana. No solo está dirigida a techies que quieran organizarse para apoyar a su movimiento, sino también a personas que quieran montar una línea de atención y que, siguiendo los pasos indicados en los capítulos iniciales, puedan planificar su creación y posteriormente buscar a otras personas con formación técnica para dotarla de personal durante la fase de implementación.

Este documento es el resultado de la trayectoria de las organizaciones que forman parte de CiviCERT y de proyectos con basta experiencia en atención a amenazas y ataques en materia de seguridad digital. Se identificaron aprendizajes, desafíos y buenas prácticas que orientarán a quienes se encuentren dando los primeros pasos en este campo. En este sentido, la guía comienza esbozando una definición sobre las líneas de atención sobre seguridad digital para la sociedad civil (LASDSC), y especificando diferencias y puntos en común entre redes de soporte, hotlines, helplines y help desks. A su vez, describe las características y funciones de los Equipo de Respuesta a Emergencias Informáticas (CERT).

Luego, el primer capítulo ofrece una serie de elementos para diseñar el marco de trabajo de la línea de atención: cómo decidir qué servicios va a ofrecer, a quién estará dirigida y qué medidas serán necesarias para prestar dichos servicios.

El capítulo 2 detalla los pasos necesarios para elaborar un plan realista para creación de la línea de atención sobre seguridad digital para la sociedad civil. Es decir, sus aspectos materiales: desde su financiación hasta la instalación de una oficina segura, pasando por la dotación de la infraestructura y la conformación y capacitación del equipo.

El capítulo 3 explica el servicio más importante que debe brindar el equipo, la gestión de incidentes. Aquí se detallan las fases y recursos necesarios para atender una solicitud de apoyo: preparación; detección y análisis; contención, erradicación y recuperación; y las acciones posteriores al incidente. También se incluyen buenas prácticas de documentación de los flujos de trabajo y los procedimientos.

Por último, el capítulo 4 va más allá del funcionamiento cotidiano de la línea de atención y ofrece recomendaciones sobre cómo y por qué colaborar con otras líneas de atención sobre seguridad digital y equipos de emergencia informática, y cómo evaluar el trabajo para asegurarse de que se presta un servicio de calidad a las beneficiarias.

También hemos incluido una serie de plantillas que se pueden utilizar para crear el marco de trabajo y las medidas necesarias para la línea de atención.

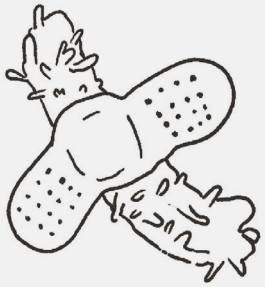
Esta guía no habría sido posible sin la existencia de CiviCERT y los aportes de sus integrantes, quienes compartieron documentación, redactaron nuevos contenidos, concedieron entrevistas y revisaron el resultado final. Nos gustaría agradecer especialmente a:

* **Access Now Helpline**, por el gran apoyo que nos han ofrecido, por compartir generosamente su documentación, tanto la pública como la confidencial y por organizar un sprint interno de redacción para ofrecer

excelentes consejos sobre cómo gestionar una LASDSC. Muchas gracias en especial a: Michael Carbone, Maggie Haughey, Mohamed Chennoufi, Rogelio López, Daniel Bedoya Arroyo y Beatrice Martini. Un reconocimiento especial a Hassen Selmi, coordinador de respuesta a incidentes de la Línea de Ayuda de Access Now, por la entrevista que nos concedió y que sirvió de base para la sección sobre el proceso de gestión de incidentes (capítulo 3).

* Daniel Ó Cluanaigh, que ayudó a contar la historia del proyecto *Field-building* del **Programa de Defensoras Digitales** para el desarrollo de capacidades comunitarias.
* Etienne Maynier, cuya entrevista sobre la publicación de información restringida en **Amnesty Tech** inspiró muchas secciones sobre la gestión de información y la comunicación con las personas beneficiarias.
* Farhanah, facilitadora de protección digital en el **Programa de Defensoras Digitales**, por redactar la versión inicial de la sección sobre documentación de procedimientos y por recopilar información para otras secciones.
* Grégoire Pouget y Jean-Marc Bourguignon, de **Nothing2Hide**, por su contribución a las secciones sobre comunicación segura y gestores de tickets, y por el entusiasmo con el que se sumaron a este proyecto en cuanto se incorporaron a CiviCERT.
* **Luchadoras**, por la entrevista que nos concedieron sobre su línea de ayuda feminista.
* Lu Ortiz, cofundadora y directora ejecutiva de **Vita Activa**, por la entrevista que nos concedió sobre el modelo de cuidados del equipo de Vita Activa.
* Mario Felaco, de **Conexo**, Alexandra Haché de **Digital Defenders Partnership**, Jannat Fazal y Shmyla Khan de **Digital Rights Foundation Pakistán**, Harlo Holmes, de **Freedom of the Press Foundation**, y Carlos Guerra, de **Internews**, por su ayuda en la concepción y coordinación de esta guía.
* Todas las líneas de atención feministas que participaron en la serie de seminarios web **"Construir infraestructura feminista: Líneas de atención feministas para personas que enfrentan violencia de género en espacios digitales"** organizados por el **Programa de Defensoras Digitales** en 2021.
* Todas las organizaciones, tanto integrantes como no integrantes de CiviCERT, que completaron el largo cuestionario que redactamos para recopilar casos prácticos para esta guía.

Esperamos que esta guía apoye la creación de líneas de atención sobre seguridad digital para la sociedad civil en todo el mundo. Por favor, envíanos tus comentarios y sugerencias sobre cómo mejorarla y mantenerla a **tech-care@digitaldefenders.org**. También puede sugerir mejoras creando un *issue* o enviando una solicitud de *merge* en este repositorio de Gitlab: **https://gitlab.com/rarenet/tech-care-gatsby**.

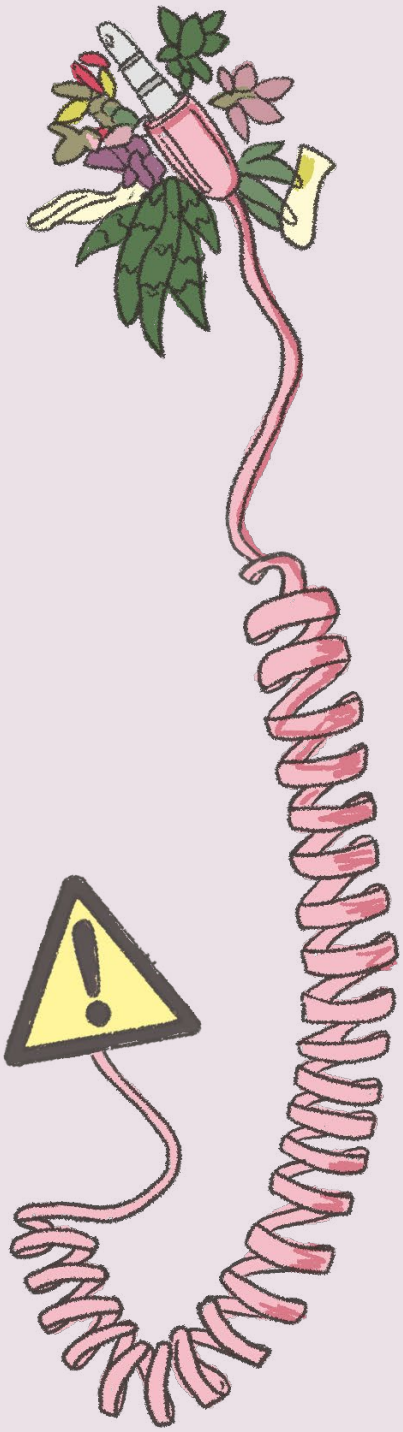


¿Qué es una línea de atención sobre seguridad digital para la sociedad civil?

La información, el apoyo y el aliento que personas desconocidas proporcionan a la distancia puede suponer un cambio decisivo en la vida de una persona, e incluso, en algunos casos, hasta salvarla. Este apoyo o asesoramiento es, en esencia, un ámbito de actuación humana que se caracteriza por su diversidad y heterogeneidad. Las razones y motivaciones que impulsan la creación de líneas de atención, y las formas en que se autodefinen y presentan a sí mismas, pueden ser muy diversas. Por ello, sus procedimientos, normas y políticas, así como sus modelos de sostenibilidad, también lo son.

Estas iniciativas pueden sumarse a acciones colectivas –de alcance local, regional, nacional o incluso internacional– que tienen el fin de construir redes de apoyo y solidaridad, como en el caso de las convergencias transnacionales entre movimientos sociales, por ejemplo. Por lo general, nacen de forma orgánica e informal a partir de la iniciativa de personas y colectivos que se organizan para brindar soluciones, servicios, cuidados y atención a los problemas que se les plantean. La participación en estas redes es voluntaria, es decir que no está motivada por un interés económico sino por el capital social o la alegría que produce participar en actividades ciudadanas o de voluntariado.

Muchas de estas iniciativas se pueden entender, por lo tanto, como una respuesta autogestionada de la sociedad civil para contrarrestar y combatir la larga serie de injusticias y violencias generadas por los sistemas capitalistas, patriarcales, racistas y coloniales en los que vivimos. Dentro de estas redes informales de apoyo y de las líneas de atención de la sociedad civil existentes encontramos muchos modelos de apoyo a la distancia. Esta sección tiene como objetivo presentarlos, definirlos y enumerar sus principales ventajas y características.



Ventajas y valor de los servicios de apoyo a distancia

En términos generales, existen una serie de clasificaciones y valores asociados a los públicos a los que las líneas de atención prestan sus servicios y a las maneras en las que lo hacen. Por ejemplo, algunas líneas de atención se definen como Líneas Voluntarias de Apoyo Emocional (**VESH**[1], por sus siglas en inglés). Estas integran una red internacional que combina los distintos servicios de asistencia telefónica de tres proyectos internacionales: Befrienders/Samaritans, IFOTES y Lifeline. En conjunto, agrupan a 1200 centros distribuidos en 61 países, que trabajan conjuntamente para promover buenas prácticas y técnicas de comunicación que favorezcan la salud emocional, incrementar el intercambio de información entre las asociaciones participantes y representar las experiencias de sus integrantes a nivel internacional.

De forma complementaria, la Federación Internacional de Servicios Telefónicos de Emergencia (**IFOTES**,[2] por sus siglas en inglés) elabora normas internacionales para dichos servicios de escucha, los cuales deben aplicar y respetar los siguientes puntos:

- Los servicios telefónicos de emergencia están disponibles, en todo momento, para cualquier persona que desee contactar, independientemente de su edad, sexo, religión o nacionalidad.
- Todas las personas que llaman tienen derecho a ser escuchadas y tratadas con respeto, independientemente de sus creencias, convicciones y opciones personales.
- Se debe escuchar con una actitud abierta y acogedora y respetar siempre la siguiente regla de oro: no imponer nunca ninguna obligación a la persona que llama.
- El contenido de una llamada es estrictamente confidencial, especialmente cualquier información relativa a la vida privada.
- Durante la conversación telefónica la persona receptora debe permanecer en estricto anonimato y la persona que llama tiene derecho a permanecer en anonimato si así lo desea.
- Los servicios trabajan de forma voluntaria. Las personas que atienden las llamadas han sido seleccionadas, formadas y supervisadas para mejorar constantemente sus habilidades de escucha.
- Los servicios telefónicos de emergencia son totalmente gratuitos para la persona que llama.

Por otro lado, el **manual de USAID sobre cómo crear una línea directa** (Stratten y Ainslie, 2003)[3] destaca las siguientes ventajas a la hora de plantearse la creación de una nueva línea:

- Las líneas directas son una forma eficaz de proporcionar información precisa y consejos y de derivar a los servicios o recursos comunitarios adecuados. El anonimato que ofrece una línea directa es una ventaja fundamental, sobre todo cuando se trabaja con adolescentes, ya que permite a quien llama hacer preguntas que pueden ser difíciles o incómodas de abordar en un entorno presencial.
- Las líneas directas pueden ser un barómetro útil para medir el impacto de las campañas de educación pública y de los medios de comunicación y pueden proporcionar información para orientar nuevas intervenciones.

1 **https://en.wikipedia.org/wiki/Volunteer_Emotional_Support_Helplines**

2 **https://www.ifotes.org/en/about**

3 **https://pdf.usaid.gov/pdf_docs/PNACU541.pdf**

- Las líneas directas refuerzan los mensajes de prevención que se difunden a través de otros canales, especialmente de los medios de comunicación de masas. Pero, a diferencia de estos, lo hacen de forma interpersonal y cercana a través de las líneas telefónicas. Es esta comunicación interpersonal la que puede lograr que la gente adopte nuevos comportamientos.

Históricamente, la gran mayoría de las líneas de atención eran por teléfono. Hoy en día suelen complementarse con otros canales como formularios de contacto, correos electrónicos, chats de servicios de mensajería instantánea, SMS e incluso *bots*. Cada formato tiene sus ventajas y desventajas en cuanto al tipo y la calidad de la interacción, así como en cuanto el tipo de atención y apoyo que se pueden ofrecer.

Como hemos indicado en esta introducción, las líneas atención pueden servir para proporcionar información precisa y rápida a las poblaciones vulnerables o en riesgo, y ofrecer una oportunidad de diálogo y mayor capacidad de comprensión de lo que estas poblaciones sienten, están viviendo y necesitan.

Líneas directas (*hotlines*), líneas de ayuda (*helplines*) y líneas de atención (*help desks*)

Existen diferentes tipos de líneas que ofrecen apoyo a la distancia. Una **línea directa**[4] es un teléfono que dirige automáticamente, sin marcar ningún número, a un destino preseleccionado. Sin embargo, el uso coloquial del término "línea directa" suele referirse a un centro de llamadas al que se accede marcando un número de teléfono concreto. Hay números gratuitos para denunciar delitos, llamar a la policía, a los bomberos y a otros servicios de emergencia. Estas líneas directas suelen estar gestionadas, apoyadas o financiadas por instituciones públicas.

Las **líneas de ayuda**[5] pueden ofrecer información general, asesoramiento especializado, acompañamiento personalizado o un servicio más genérico de escucha y apoyo emocional.

Hay organizaciones de la sociedad civil que ofrecen líneas directas y líneas de ayuda para prevenir el suicidio, apoyar a personas que sufren violencia y distintas formas de discriminación, denunciar delitos o prestar apoyo inmediato tras una catástrofe natural o humanitaria (guerra, terrorismo, etc.).

Estos servicios pueden ser gratuitos o de pago, temporales o permanentes, gestionados por organizaciones locales sin fines de lucro o por ONG y entidades que trabajan en el campo de la cooperación internacional. Algunas líneas directas y de ayuda atienden las 24 horas, siete días por semana, mientras que otras tienen un horario más limitado.

Es importante tener en cuenta que, aunque los términos "línea directa" y "línea de ayuda" se utilizan a menudo indistintamente, en algunos casos sí se distinguen por tener objetivos claramente diferenciados. A veces el concepto de línea directa está más orientado a líneas temporales para aliviar situaciones de crisis relacionadas con catástrofes naturales o humanitarias y tiende a coincidir en estos casos con el concepto de línea de crisis. En estos casos, el concepto de línea directa se utiliza más en el contexto de las ONG y de la cooperación al desarrollo.

En otros casos, hemos identificado iniciativas que utilizan ambos conceptos para diferenciar ante su público los servicios que ofrecen. Por ejemplo, **SaferNet**,[6] un proyecto fundado en 2005 en Brasil, está claramente dividido entre la línea directa,

4 **https://en.wikipedia.org/wiki/Hotline**

5 **https://new.safernet.org.br/helpline**

6 **https://new.safernet.org.br/denuncie**

que sirve para denunciar delitos en internet, y la línea de ayuda, que ofrece apoyo a las personas que enfrentan violencia en internet.

Además de estos ejemplos, también encontramos la noción de **línea de atención**[7], iniciativas con la finalidad de brindar información y apoyo sobre los productos y servicios de una empresa o institución. El propósito de una línea de atención, por lo general, es resolver problemas o proporcionar orientación sobre productos o servicios. También pueden centrarse en proporcionar respuestas y soluciones para los problemas o emergencias que puedan surgir del uso y la interacción con las TIC: desde dispositivos electrónicos, *software*, *hardware*, infraestructura de telecomunicaciones, administración de redes, plataformas de redes sociales, etc.

Creemos que el concepto de Línea de Atención sobre Seguridad Digital para la Sociedad Civil (LASDSC), que por lo general suelen ser adoptado por proyectos que proporcionan apoyo a activistas, personas defensoras de los derechos humanos, u organizaciones de la sociedad civil que enfrentan riesgos, ataques y emergencias digitales, tiene un interés central para esta guía. Resulta difícil rastrear sus orígenes con precisión, pero podemos nombrar algunas iniciativas que entendemos que forman parte de su trayectoria.

Por ejemplo, los hacklabs, "son espacios o edificios donde personas interesadas en la tecnología se reúnen para socializar, crear o compartir conocimientos y trabajar en proyectos de forma individual o en equipo" (**Maxigas, 2014**)[8]. Los *hacklabs* son espacios organizados por hackers y para hackers, donde personas interesadas en hackear las Tecnologías de la Información y la Comunicación, desarrollar tecnologías libres y debatir sobre las implicaciones políticas de la tecnología pueden reunirse y reconocerse. Estos espacios permiten que las comunidades de hackers prosperen y pongan sus habilidades y conocimientos técnicos al servicio de otros movimientos y colectivos sociales, en especial a la hora de crear infraestructuras de información y telecomunicaciones autónomas, aprender a utilizarlas de forma más segura y facilitar el uso de las TIC para informar, comunicar y documentar sus luchas.

El colectivo hacktivista **Telecomix**[9], por ejemplo, apoyó a activistas en Egipto a eludir la censura estatal de internet mediante el uso de teléfonos fijos. También podemos encontrar ejemplos de hackers apoyando a movimientos sociales en las colectivas ciberfeministas que han acompañado a otras colectivas feministas a mitigar y combatir la violencia de género y a migrar hacia infraestructuras tecnológicas más seguras.

La proliferación de ataques digitales dirigidos a activistas, personas defensoras de derechos humanos y organizaciones de la sociedad civil con el objetivo de dificultar o impedir su trabajo ha sido una tendencia creciente en la última década y ha motivado la conformación de líneas de atención sobre seguridad digital. Por ejemplo, **Access Now Digital Security Helpline**[10], creada en 2014, es una de las primeras de este tipo cuyos servicios están orientados explícitamente a la sociedad civil.

Los orígenes de las líneas de atención sobre seguridad digital para la sociedad civil están vinculados a iniciativas informales como los *hacklabs* y a los movimientos hacktivistas, que parten de redes descentralizadas con una afiliación flexible. Sin embargo, en general, se organizan en base a normas y políticas formales que definen las formas en que prestan apoyo, documentan su trabajo y comparten información sensible con otros proyectos. Para entender este nivel de formalización, debemos introducir el concepto de Equipo de Respuesta a Emergencias Informáticas (CERT, por sus siglas en inglés).

7 **https://en.wikipedia.org/wiki/Help_desk**

8 **https://www.coredem.info/rubrique48.html**

9 **https://en.wikipedia.org/wiki/Telecomix**

10 **https://www.accessnow.org/help**

CERT, CSIRT y SOC

Un Equipo de Respuesta a Emergencias Informáticas (**CERT**)[11] "funciona siguiendo protocolos muy específicos para determinar cómo se gestionan y documentan los incidentes informáticos, cómo se coordinan las acciones de mitigación, alerta y seguimiento con otras entidades u organizaciones y qué pautas deben seguirse para compartir información (casi siempre de carácter sensible y confidencial) con otras personas y organizaciones".

El primer CERT© o CERT-CC fue creado en 1988 por el Software Engineering Institute para responder y mitigar los problemas creados por el **Gusano Morris**[12]. Aunque el término CERT fue patentado por este instituto, se permite su uso por otros proyectos e iniciativas. Sin embargo, también se utilizan otros términos como CSIRT (Equipo de Respuesta ante Incidencias de Seguridad Informáticas), CIRT (Equipo de Respuesta ante Incidencias de Informáticas), o SIRT (Equipo de Respuesta de Seguridad Informáticas, SIRT, por sus siglas en inglés), entre otros.

Los CERT pueden crearse a nivel de una empresa, un Estado, un sector de infraestructuras clave o un grupo de organizaciones. Estos suelen proporcionar un conjunto de servicios que van desde la gestión de la información y de incidentes de ciberseguridad, hasta la supervisión de la seguridad digital, la gestión y el seguimiento de l as vulnerabilidades y la gestión general del intercambio de conocimientos sobre ciberseguridad. Los CERT nacionales también suelen denominarse Centros Nacionales de Ciberseguridad (CNS, por sus siglas en inglés), que, además de cumplir las funciones de un CSIRT, prestan servicios adicionales como la gestión de los sistemas de clasificación de la información dentro de un país.

Por último, es preciso mencionar a los Centros de Operaciones de Seguridad (SOC, por sus siglas en inglés), que proporcionan un servicio de detección de incidentes mediante la supervisión de redes y sistemas y que también pueden ocuparse de la respuesta y la gestión de incidentes (**ENISA**, **2020**)[13]. Por lo general, en las grandes empresas los SOC se centran en los servicios de supervisión y detección exclusivamente, y transfieren la gestión de incidentes a un CSIRT independiente. En las organizaciones más pequeñas, las funciones de los CSIRT y los SOC suelen solaparse.

De acuerdo con el manual de referencia desarrollado por el CERT nacional neerlandés (**FIRST**, **2006**)[14], estas son algunas de las ventajas de crear un CERT:

- Establecen un punto de coordinación central para la seguridad de las TIC dentro de su organización.
- Responden de forma sistemática a los incidentes TIC y toman las medidas apropiadas.
- Ayudan a su sector a recuperarse rápida y eficazmente de los incidentes de seguridad y a minimizar la pérdida o el robo de información y la interrupción de los servicios.
- Utilizan la información obtenida durante la gestión de incidentes para prepararse mejor para la gestión de futuros incidentes y ofrecer una mejor protección de sistemas y datos.
- Se ocupan adecuadamente de las cuestiones jurídicas que puedan surgir durante los incidentes.
- Procuran intercambiar conocimientos dentro de su sector.

11 **https://en.wikipedia.org/wiki/Computer_emergency_response_team**

12 **https://en.wikipedia.org/wiki/Morris_worm**

13 **https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc**

14 **https://www.first.org/resources/guides/cert-in-a-box.zip**

Redes internacionales como **FIRST** [15] y **Trusted Introducer**[16] reúnen a varios equipos de respuesta a incidentes de seguridad informática de organizaciones gubernamentales, comerciales o educativas. El objetivo de estas redes es fomentar la cooperación y la coordinación en la prevención de incidentes, facilitar la reacción rápida y promover el intercambio de información entre sus integrantes y la comunidad en general. También crean normas y protocolos para garantizar la correcta certificación de los CERT.

Aunque históricamente los CERT se han centrado en responder a las necesidades de grandes empresas, universidades e incluso países enteros, *modus operandi* también puede servir para la sociedad civil, ya sean personas que defienden los derechos humanos, activistas, organizaciones sin fines de lucro o la ciudadanía en general, que son objeto de ataques y emergencias cada vez más frecuentes en los espacios digitales.

CiviCERT

El Centro de Respuesta a Incidentes Informáticos de la Sociedad Civil (**CiviCERT**)[17] se creó en 2015. En 2016, CiviCERT se convirtió en miembro oficial de la red *Trusted Introducer*, un paso necesario para ser reconocido como CERT. Algunas personas que forman parte de CiviCERT a nivel individual, también forman parte de FIRST. Estas acreditaciones proporcionan una plataforma única para presentar cuestiones de seguridad digital importantes que afectan a la sociedad civil a un amplio espectro de CERT que prestan servicio a entidades gubernamentales y empresariales.

La **política de afiliación y el código de conducta, así como las políticas de gestión de datos e información y de verificación de CiviCERT**[18] se diseñaron para adaptarse mejor a las realidades de las organizaciones y personas que se fueran a unir a este proyecto. En 2022, CiviCERT contaba con 30 organizaciones y tres personas a nivel individual. Cerca de la mitad de sus integrantes son organizaciones internacionales como Access Now, Amnesty International Security Lab, Digital Defenders Partnership, Freedom of the Press Foundation, Front Line Defenders, Human Rights Watch, Internews y Organised Crime and Corruption Reporting Project, quienes realizan un trabajo extenso de supervisión, investigación e incidencia política a escala internacional en cuanto a violaciones de derechos humanos y derechos digitales y, en algunos casos, también proporcionan financiación, respuesta rápida y acompañamiento y formación en materia de seguridad digital.

La otra mitad consiste en proyectos que trabajan en un país o a nivel regional y proporcionan una respuesta rápida, ya sea como línea de atención, o proporcionando formación y acompañamiento o análisis y documentación sobre *software* malicioso (*malware*) y otras amenazas digitales. Entre los países representados se encuentran Armenia, Brasil, Colombia, Estados Unidos, Luxemburgo, Myanmar, Nigeria, Pakistán, Serbia, Taiwán, Tíbet, Uganda y Ucrania.

Los miembros de CiviCERT comparten entre sí actualizaciones sobre los casos de respuesta rápida que acompañan, el tipo de riesgos o amenazas nuevas que afronta la sociedad civil y los recursos, investigaciones o herramientas que se están desarrollando. En conjunto, estas actualizaciones proporcionan una instantánea del panorama mundial de ataques digitales contra los movimientos sociales y la sociedad civil. Asimismo, se brinda apoyo en cuanto a conocimientos o acceso a recursos. En la medida de lo posible, se organizan seminarios en línea para presentar casos o metodologías específicas.

15 **https://www.first.org/**

16 **https://www.trusted-introducer.org/**

17 **https://civicert.org**

18 **https://www.civicert.org/policies/**

Las organizaciones que integran CiviCERT se coordinan a través de una lista de correo privada y cifrada, y se reúnen en encuentros presenciales, ya sea en conferencias internacionales sobre seguridad digital para la sociedad civil o en eventos de formación para sus miembros. Al ser parte de CiviCERT se tiene acceso a una serie de recursos e infraestructura técnica compartida.

Por ejemplo, las organizaciones de CiviCERT que lo deseen pueden figurar como organización de apoyo en el **Kit de Primeros Auxilios Digitales**[19], un recurso gratuito para ayudar a quienes ofrecen respuesta rápida a incidentes, a formadoras en seguridad digital y a activistas que quieran aprender a protegerse mejor, tanto a sí mismas como a sus comunidades, contra las emergencias digitales más comunes. Este recurso actúa como mecanismo de admisión de las solicitudes de apoyo a CiviCERT mediante un enfoque tipo "elige tu propia aventura" que guía al visitante a través de varias preguntas para entender cuál es su problema y qué miembro de CiviCERT puede resolver mejor su emergencia. El sitio web, que también puede utilizarse sin conexión, está disponible en albanés, árabe, birmano, español, francés, indonesio, inglés, portugués, ruso y tailandés.

Además, los miembros de CiviCERT tienen acceso a una instancia de la **Malware Information Sharing Platform** (**MISP**[20]), al proyecto **Phishdetect**[21] y a otra instancia de **Cuckoo Sandbox**[22] que facilita el análisis forense de software malicioso, analizando qué hace, a qué componentes afecta y qué conexiones realiza.

CiviCERT y las líneas de atención sobre seguridad digital para la sociedad civil siguen siendo una excepción y los modelos actuales de CERT/CSIRT/SOC no suelen desarrollarse pensando en la ciudadanía y en la sociedad civil. En general, están orientados principalmente al sector comercial y gubernamental y no tienen una perspectiva interseccional en su análisis de los riesgos a los que se enfrentan los públicos a los que prestan servicio, sino que tienden a promover una visión apolítica y neutral de las tecnologías.

Este escenario puede generar graves problemas, ya que los institutos de ciberseguridad que cuentan con financiación pública solo dan prioridad a entidades comerciales y a menores, ignorando los riesgos a los que se enfrentan las mujeres, las personas LGBTQIA+ y las poblaciones históricamente discriminadas y marginadas, todas ellas a menudo objeto de fraudes electrónicos, ciberdelitos y violencia de género que estas organizaciones no suelen atender ni trabajar. La carga de contrarrestar estos peligros, riesgos y violencia recae, por lo tanto, en la sociedad civil organizada, que recibe financiación y apoyo limitados.

19 https://digitalfirstaid.org/

20 https://www.misp-project.org/

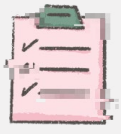
21 https://github.com/phishdetect

22 https://cuckoosandbox.org/

Diseña tu marco de trabajo

Crear un marco para la Línea de Atención sobre Seguridad Digital para la Sociedad Civil (LASDSC) permitirá describir en detalle qué función tendrá, cuál será el público al que se dirigirá, qué diseño organizacional tendrá y con quién cooperará. Este ejercicio sirve también para hacerse una idea de los recursos que se necesitarán para apoyar a sus beneficiarias. Es importante invertir el tiempo que sea preciso para el diseño de este marco, ya que sentará las bases de la línea de atención.

Este capítulo describe cómo identificar al público beneficiario y analizar sus necesidades, definir su misión y entorno, establecer los servicios básicos y los parámetros de comunicación, y especificar sus políticas. Las LASDSC pueden ser muy diferentes entre sí, por lo que cada una tendrá un marco diferente. Sin embargo, los elementos descritos en este capítulo pueden aplicarse a todo tipo de proyectos.



Pueden usar la plantilla de marco de trabajo en la página 69 para facilitar el proceso

Descarga la plantilla de marco de trabajo en
https://tech-care.cc/es/06-framework-template

1.1 Define tu público

En esta guía se utilizará el término "público" para definir el conjunto de personas beneficiarias atendidas por una LASDSC. Asimismo, se denominará "beneficiaria" cuando se trate de una sola persona u organización.

A la hora de poner en marcha una LASDSC es esencial tener una visión clara de quiénes serán sus beneficiarias y el tipo de entorno para los que se van a desarrollar sus servicios. La decisión sobre a quién prestar servicio o no puede depender de la misión de su organización, de las políticas de las entidades financiadoras, de consideraciones legales o incluso de un escenario político cambiante que pone en riesgo a un grupo específico de personas.

En términos generales, se supone que las LASDSC están dirigidas a la sociedad civil o a una parte de ella. Aun así, teniendo en cuenta que la definición de "sociedad civil" varía mucho según el grupo o sector, puede resultar útil ofrecer una lista de los tipos de beneficiarias a los que actualmente prestan servicio las LASDSC que integran CiviCERT:

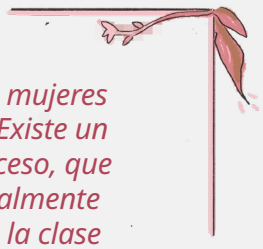
- Activistas
- Organizaciones no gubernamentales
- Personas defensoras de los derechos humanos
- Organizaciones de derechos humanos amenazadas
- Medios de comunicación independientes
- Organizaciones indígenas
- Periodistas
- Personas que defienden la tierra
- Grupos LGTBIQA+
- Mujeres
- Jóvenes

1.2 Analiza las necesidades de tu público

Identificar y evaluar las necesidades y expectativas del público al que se dirigen y el contexto en el que operan será fundamental para el éxito del proyecto. Deben hablar con su público acerca del valor real que podría aportar su LASDSC, analizando las amenazas a las que podrían enfrentarse sus beneficiarias y sus necesidades respecto a los incidentes de seguridad digital y la prevención de amenazas. Esto puede hacerse de forma presencial o a distancia, en grupos o en entrevistas individuales, tanto de forma pública como privada.

Hay varios marcos de trabajo que pueden utilizarse para este tipo de análisis. Los dos más comunes son:

- **FODA:** para identificar las debilidades, amenazas, fortalezas y oportunidades.
- **PESTEL:** para incorporar la dimensión política, económica, social, tecnológica, ecológica y legal en el análisis contextual.



Trabajamos con mujeres de todo el país. Existe un problema de acceso, que está fundamentalmente relacionado con la clase y la edad. En general, no solemos recibir peticiones de mujeres jóvenes y de clase media porque ellas mismas consiguen resolver sus problemas de violencia de género gracias a las TIC. Luego, hay personas mayores, niñas y niños y adolescentes de zonas rurales que recién comienzan su relación con las TIC. También apoyamos a personas con un perfil público a quienes se les agrede constantemente y que también necesitan estrategias específicas... periodistas, mujeres políticas o con cargos públicos y activistas. Así que, para cada uno de estos grupos, tenemos una forma distinta de abordar el trabajo y la violencia a la que se enfrentan.

SOS Digital (Haché, 2021).

Estuvimos trabajando para crear conocimiento sobre cómo las mujeres estaban viviendo la violencia en México, para poder identificarla y también reconocerla. Y nuestro trabajo era hacer visible la violencia en la agenda pública, esto nos convirtió en un referente y también se abrió una posibilidad de tener un espacio de apoyo para las mujeres que estaban enfrentando esta violencia. Comienzan a llegar solicitudes y en marzo de 2020 decidimos equipparnos y acuerpar a otras mujeres que nos estaban buscando para pedirnos apoyo, acompañamiento e información.

Luchadoras (Haché, 2021).

Una vez hayan analizado las necesidades de su público, una buena práctica es realizar una actividad de simulación de amenazas para analizar las características del contexto político en el que van a trabajar, identificar las vulnerabilidades y amenazas de la línea de atención, así como la probabilidad de que se produzcan y especificar los requisitos de prevención y mitigación. Este modelo de amenazas debe tenerse en cuenta a la hora de desarrollar las políticas de la línea de atención, los procedimientos técnicos, la documentación y la formación del personal.

Encontrarás en la página 69 la plantilla de marco de trabajo ofrecemos algunas claves para realizar estos análisis. Descárgala en **https://tech-care.cc/es/06-framework-template**

Para saber más

Higson Smith, Craig, Ó Cluanaigh, Daniel, Ravi, Ali G., Steudtner, Peter. (2016). Overall Framework for Context Analysis. *Holistic Security - A Strategy Manual for Human Rights Defenders*. Tactical Technology Collective. **https://holistic-security.tacticaltech.org/chapters/explore/2-1-overall-framework-for-context-analysis.html**

Front Line Defenders (2011). Understanding Your Context. *Workbook on Security: Practical Steps for Human Rights Defenders at Risk*, pp. 61-7.

Schulte, Jennifer (2018). Gender-Based Risk Model. *Cyberwomen: Holistic Digital Security Training Curriculum for Women Human Rights Defenders.* Institute For War and Peace Reporting. **https://iwpr.net/global-voices/print-publications/cyberwomen-holistic-digital-security-training-curriculum-women**

1.3 Define tu misión

Después de analizar las necesidades y el contexto de su público, el siguiente paso de planificación debe ser la redacción de una declaración de misión que explique claramente el propósito y la función de la LASDSC y proporcione una breve descripción de las metas principales del proyecto.

Como esta será la base sobre la cuál va a trabajar la LASDSC durante algunos años, una buena práctica es no caer en ambigüedades y redactar una declaración de misión concisa, pero no demasiado breve.

He aquí dos ejemplos de declaraciones de integrantes de CiviCERT:

Línea de Ayuda en Seguridad Digital de Access Now

Access Now defiende y refuerza los derechos digitales de las personas usuarias en peligro en todo el mundo. Combina apoyo técnico directo, el compromiso con una política integral, incidencia política a nivel global, la concesión de subvenciones y encuentros como RightsCon, para luchar por los derechos humanos en la era digital.

Combatimos y cuestionamos la industria de la vigilancia y la persecución de activistas a través de apoyo a la seguridad digital, investigación, incidencia política y campañas. En Amnesty Tech, cada equipo tiene que definir el problema que quiere abordar y crear una estrategia de cambio. Nos preguntamos: "¿Cómo podemos cambiar esto?" Y esta pregunta nos lleva a muchos debates, por lo que nos centramos más en la investigación. Mientras que Access Now y otras organizaciones proporcionan apoyo digital a un público amplio, aquí nos centramos en las personas que son o han sido objeto de vigilancia. Realizamos tanto investigaciones como apoyo a la seguridad digital.

Etienne Maynier, Amnesty Tech (Entrevista, Diciembre 2021).

La Línea de Ayuda en Seguridad Digital de Access Now proporciona soluciones tecnológicas y asesoramiento a tiempo real para personas que se encuentran en una situación de riesgo en contextos en los que las comunicaciones no son abiertas, libres o seguras. A través de nuestra línea de ayuda para la seguridad digital, que funciona 24 horas al día, 365 días al año, ofrecemos asesoramiento técnico y respuesta a incidentes para brindar información y apoyo a activistas, periodistas, personas que defienden los derechos humanos y personas o entidades de la sociedad civil sobre el terreno.

Las metas y objetivos principales de la Línea de Ayuda en Seguridad Digital de Access Now son:

- Proporcionar apoyo técnico directo a personas y organizaciones en situación de riesgo para identificar y abordar sus necesidades de seguridad digital.
- Proporcionar asistencia a personas y organizaciones en situación de riesgo para proteger sus activos digitales, comunicaciones y otras actividades en línea y ayudarles a eludir la censura y obtener acceso a los servicios que necesitan.
- Proporcionar conocimientos técnicos, apoyo y coordinación para prevenir y detener infecciones de software malicioso y abordar las vulnerabilidades de los sistemas y el software.
- Mantener a nuestro público al día sobre las nuevas amenazas y vulnerabilidades que deben abordarse urgentemente.
- Coordinar el apoyo a personas en situación de riesgo cuando este apoyo pueda ser proporcionado de forma más adecuada por otros CERT.
- Convertirse en un centro de referencia por su excelencia en seguridad de la información al que puedan recurrir organizaciones nacionales e internacionales.

Mnemonic

Mnemonic trabaja en todo el mundo para ayudar a las personas que defienden los derechos humanos a documentar eficazmente de forma digital las violaciones de derechos humanos y los crímenes internacionales, a fin de apoyar la incidencia política, la justicia y la rendición de cuentas.

Nuestros objetivos son:

- Archivar la información digital para garantizar que las posibles pruebas no se pierdan y permanezcan accesibles y utilizables para futuros mecanismos de imputación.

- Formar a las personas defensoras de derechos humanos para maximizar el impacto de la información digital y empoderar a quienes trabajan con ella.
- Reducir el impacto de las políticas de moderación de contenidos perjudiciales por parte de empresas de redes sociales y gobiernos, proporcionando datos exhaustivos y fiables sobre la retirada de documentación de derechos humanos de las plataformas de redes sociales.
- Crear y apoyar el desarrollo de herramientas y métodos de código abierto para aumentar la capacidad de las personas que defienden los derechos humanos de utilizar la información digital para promover la justicia social.

La línea de ayuda actúa como puente. Cuando es necesario, derivamos nuestros casos a las plataformas de redes sociales, ya que tenemos comunicación directa con Facebook y su programa piloto "No sin mi consentimiento". También derivamos casos al programa piloto de Internet Watch Foundation sobre pornografía infantil en línea y les trasladamos peticiones de retirada de contenido nocivo. A veces apoyamos a denunciantes que presentan una denuncia ante las autoridades en Pakistán. O ponemos en contacto a mujeres y niñas que quieren huir de familias tóxicas o de relaciones abusivas con centros de acogida en Pakistán. Todo esto va más allá de los servicios de seguridad digital y la asistencia jurídica que ofrece la línea de ayuda.

Digital Rights Foundation (Haché, 2021).

1.4 Define tu diseño organizacional

A la hora de planificar la creación de una LASDSC, es preciso tomar decisiones sobre su diseño organizacional: ¿formará parte de una organización más grande o se gestionará de forma independiente? ¿Necesitará recaudar fondos por su cuenta o cuenta con un departamento de recaudación de fondos que le proporcionará recursos?

La LASDSC puede tener distintos diseños organizacionales. Muchas son proyectos de organizaciones sin fines de lucro más grandes o trabajan dentro de un proveedor de servicios de Internet para la sociedad civil. Otras son independientes y algunas funcionan con voluntariado. También es posible que existan múltiples capacidades de gestión de incidentes dentro de una misma organización matriz, por ejemplo, que tengan un departamento que atienda al personal de la organización y se ocupe de los incidentes de su infraestructura, mientras que otro atiende a un público externo. Algunos CERT nacionales pueden incluir entre sus servicios la gestión de incidentes de seguridad digital que afectan a organizaciones sin fines de lucro.

1.5 Define tus servicios básicos

Una LASDSC puede ofrecer muchos servicios diferentes, pero mientras proporcione algún tipo de respuesta a incidentes de seguridad digital no necesita hacerlo todo y puede centrarse en un pequeño conjunto de servicios básicos, por ejemplo, en la seguridad de las cuentas de las redes sociales u ofrecer recomendaciones sobre cómo sortear la censura en un área específica.

Muchas LASDSC prestan tanto servicios reactivos (que responden a incidentes de seguridad digital) como preventivos (iniciativas de educación en seguridad digital para

reducir el riesgo de incidentes) pero en la mayoría de los casos limitarán su lista de servicios en función de su capacidad y derivarán a otros equipos los servicios adicionales.

A continuación, ofrecemos una lista de servicios tanto reactivos como preventivos que ofrecen los miembros de CiviCERT, incluidos algunos que no son del ámbito de la seguridad digital:

Reactivo	**Preventivo**	**No estrictamente relacionado con la seguridad digital**
· Triaje inicial · Apoyo digital 24/7 · Sustitución de equipos · Gestión de vulnerabilidades y software malicioso · Gestión del hackeo de cuentas · Mitigación del acoso en línea · Análisis forense · Elusión de censura	· Formación presencial · Consultorías de seguridad organizativa · Alojamiento seguro de sitios web · Protección de sitios web · Protección contra la denegación de servicio · Evaluación de amenazas y riesgos · Protección de las comunicaciones · Seguridad de los dispositivos · Seguridad para la navegación web · Seguridad para cuentas	· Subvenciones y financiación · Reubicación de personas en riesgo · Seguridad física · Apoyo jurídico · Apoyo psicosocial · Incidencia política

1.6 Comunícate con tu público

Definir las formas en las que la LASDSC establecerá la comunicación con su público es un elemento crucial de este marco de trabajo. Tendrán que decidir cómo se pondrán en contacto su público, su disponibilidad y tiempo de respuesta y tener claro cómo se comunicarán con personas que puedan estar emocionalmente traumatizadas.

Decide cómo se pondrá en contacto tu público

Tendrán que identificar los mejores canales de comunicación para que las beneficiarias obtengan apoyo de la línea de ayuda o de la línea de atención.

Entre las cosas que deben tener en cuenta, basándose en el análisis inicial de contexto y el modelo de amenazas, es si las personas beneficiarias pueden necesitar un cifrado de extremo a extremo o un mecanismo de entrada anónimo para empezar. Si este es el caso, piensen en todos los métodos posibles para intercambiar cualquier información sensible a través de un canal seguro.

Recomendamos que establezcan al menos dos formas diferentes de contactar con su línea de atención:

* Un canal accesible para cualquier persona sin conocimientos técnicos, como una dirección de correo electrónico.
* Un canal seguro para las personas que tienen los conocimientos técnicos necesarios para utilizarlo, como un correo electrónico cifrado o una app de mensajería segura como Signal.

Estamos operando una línea de apoyo en Luchadoras para atender principalmente a mujeres que están viviendo violencia digital en México. Esta iniciativa surge a partir de un incremento en la necesidad detectada en la recepción de solicitudes recibidas en nuestras redes sociales. La línea de apoyo tiene como acciones principales: proporcionar un acompañamiento integral; primeros auxilios psicológicos; detectar necesidades o proporcionar información: alternativas de acción, formas de reporte, contenidos sobre violencia digital, seguridad digital, contactos de posibles redes de apoyo; escalamiento de casos a través de la elaboración y seguimiento de reportes en diversas plataformas; canalización a organizaciones o instituciones especializadas para un acompañamiento y seguimiento óptimo.

Luchadoras (Haché, 2021).

Garantizar la seguridad de las comunicaciones es importante. Sin embargo, la prioridad es garantizar que la LASDSC sea fácil de localizar. Por eso es importante ofrecer varios canales de comunicación. Multiplicar los canales de comunicación no tiene por qué ser necesariamente un problema siempre que el equipo esté adecuadamente organizado para compartir la información.

A continuación, ofrecemos una lista de todas las herramientas de comunicación que ofrecen los miembros de CiviCERT como posibles métodos para establecer un primer contacto con su LASDSC:

- Formulario web anónimo
- Correo electrónico
- Correo electrónico cifrado con PGP
- Teléfono
- Correo postal
- Signal
- Skype
- Telegram
- Formulario web
- WhatsApp

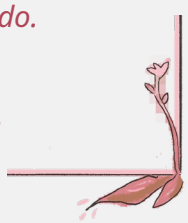
También hay que tener en cuenta que algunas de las personas beneficiarias pueden haber pasado por situaciones traumáticas y pueden requerir una escucha activa y empatía, lo que se puede ofrecer mejor a través de una llamada telefónica o una videollamada.

Existen muchas posibilidades de mantener la relación con las beneficiarias y recibir sus comentarios y aportaciones, por ejemplo:

- Foros
- Listas de correo y otros espacios comunitarios
- Reuniones, conferencias, talleres, presentaciones (presenciales y en remoto)
- Boletines informativos
- Redes sociales

En cuanto a la comunicación, lo principal para nosotras es poner sus necesidades en el centro, tratando de desactivar la culpa, acogiendo sus sentimientos, evitando la revictimización. La comunicación de Luchadoras está pensada para que sientan como si fuera una amiga que responde, que asume y secunda la decisión que toman sobre la situación por la que están pasando.

Luchadoras (Entrevista, Enero 2022).



Establece tu disponibilidad y tiempo de respuesta

Los tiempos de respuesta deben comunicarse con claridad a las personas beneficiarias para evitar falsas expectativas y para establecer un Acuerdo de Nivel de Servicio (ANS) adecuado con su público. Responder a tiempo durante la gestión de las incidencias es crucial, tanto para resolver el problema al que se enfrentan como para la reputación de la LASDSC.

La disponibilidad y el tiempo de respuesta de la LASDSC dependerán en gran medida de la plantilla y el horario de trabajo.

A menos que su LASDSC esté disponible las 24 horas del día, tendrán que decidir cómo se pueden notificar los incidentes fuera del horario de oficina. Se puede optar por revisar todos los mensajes entrantes el siguiente día laborable, o puede haber una persona del equipo de guardia para supervisar las solicitudes entrantes y decidir sobre su urgencia.

Hemos introducido los conceptos de apoyo emocional y empático en nuestra línea de ayuda. Nuestros primeros auxilios psicológicos están basados en tres preguntas: "¿Cómo llevas este estrés?" (para compartir nuestra profunda preocupación por su bienestar); "¿Puedes explicarme el problema?" (para que sean las propias personas las que controlen su relato); y "¿Qué quieres que hagamos por ti? ¿Cuál es tu deseo?" (para construir soluciones de forma conjunta con la persona que busca apoyo).

Vita Activa (Haché, 2021).

Intentamos publicar todos los datos posibles: indicadores, metodología, etc. Por ejemplo, con Pegasus también publicamos rastros forenses detallados. Cuanto más publiquemos, más posibilidades habrá de que otras personas puedan desarrollar su propia investigación, pero también menos presiones recibiremos para dar más datos, por parte de los gobiernos, por ejemplo. Luego publicamos informes técnicos detallados, de modo que, si un gobierno se dirige a nuestra organización, podemos decir: "Todo es público". Esa es una de las políticas de Amnesty Tech: publicar pruebas para tratar de evitar que nos pidan información privada.

Etienne Maynier, Amnesty Tech (Entrevista, Diciembre 2021).

Para tomar esta decisión, es importante tener en cuenta el contexto: por ejemplo, si la financiación es limitada, es posible que no se pueda pagar a una persona para que trabaje fuera del horario habitual. Estas son consideraciones importantes también para la seguridad psicosocial del equipo. Si, por ejemplo, la LASDSC está gestionada por personas voluntarias, pueden estar dispuestas a aceptar solicitudes a cualquier hora del día o de la noche, pero esto podría conducir muy rápidamente a un desgaste de las más dedicadas.

Para saber más

Para profundizar sobre la forma de cuidar el bienestar del equipo de una LASDSC, se puede consultar la sección sobre políticas de cuidados en el capítulo 2.

Define los protocolos y el tono de la conversación

Además de garantizar la confidencialidad de las comunicaciones con las personas beneficiarias, a la hora de responder a las solicitudes de apoyo las LASDSC deben tener siempre presente que estas pueden estar traumatizadas emocionalmente por la agresión que han sufrido.

He aquí algunos consejos sobre cómo establecer la comunicación con una persona que ha sufrido una agresión:

- Registrar la comunicación, comprobar si ya se han registrado comunicaciones similares.
- Utilizar un enfoque respetuoso, con una perspectiva interseccional.
- Poner a la persona solicitante en el centro, desactivando cualquier sentimiento de culpabilidad y aceptando sus sentimientos.
- Evitar la revictimización.
- Aceptar y asumir la decisión que tomen en la situación que están viviendo.

Es importante tener en cuenta distintos aspectos de contextos diferentes y escuchar los casos que llegan desde una mirada abierta y sin juicios de valor.

Para saber más

Protocolo de Access Now para gestionar casos en los que parece que la persona solicitante está sufriendo paranoia. **https://communitydocs.accessnow.org/356-paranoia_protocol.html**

1.7 Define tus políticas

Las políticas de una LASDSC son un conjunto de acuerdos y pautas que organizan el flujo de trabajo y establecen los procedimientos y protocolos estándar. Cada LASDSC precisará de unas políticas que respondan a sus necesidades específicas en función de su misión, tamaño, estructura y servicios. En esta sección se describen las políticas básicas que han adoptado distintas LASDSC, junto con plantillas que se puede utilizar para crear una LASDSC:

- Política de gestión de la información
- Plan de respuesta a incidentes
- Política de verificación
- Código de conducta
- Procedimientos operativos estándar para LASDSC

Una vez elaboradas y puestas en práctica, las políticas deben revisarse de forma periódica para verificar que siguen siendo válidas para la estructura, los procedimientos, las necesidades y las capacidades de las LASDSC con el paso del tiempo.

Amnesty Tech tiene una política de consentimiento estricta, por lo que no podemos publicar nada sin el consentimiento de la persona beneficiaria, ni siquiera de forma anónima. Tenemos que seguir una política estricta, analizando conjuntamente los riesgos y demás. Y en este punto, si el caso es reactivo y no surge de un proyecto que hayamos iniciado antes, empezamos a pensar en la estrategia de cambio: ¿Qué sabemos? ¿Qué podemos probar? ¿Qué podemos hacer para cambiar esto? De modo que, normalmente, nos reunimos para analizar cuál sería el plan de incidencia, si hay algún margen para llevar a cabo una campaña, si hay que trabajar con el equipo del país, cuál sería el riesgo de publicar la información y cuál sería el beneficio.

Etienne Maynier, Amnesty Tech (Entrevista, Diciembre 2021).

Política de gestión de la información

Cada LASDSC requiere una política de gestión y protección de la información que tenga en cuenta los procesos y procedimientos operativos y administrativos internos, así como la legislación y las normas. Por ello, es conveniente contar con la participación de una asesoría jurídica a la hora de elaborar la política de gestión de la información.

Las preguntas más básicas a las que debe responder la política de gestión de la información son:

1. ¿Cómo se "etiqueta" o "clasifica" la información?

La mayoría de las LASDSC, así como CiviCERT, clasifican la información basándose en el **Information Sharing Traffic Light Protocol (TLP)** [Protocolo de Semáforo]:

Consideramos que es importante contar con ciertos protocolos de seguridad. Un protocolo fundamental es que todas las personas que trabajan en la línea de ayuda cumplan un acuerdo de confidencialidad para garantizar la protección de la intimidad y la privacidad y que los datos que guardamos no se puedan identificar con ninguna persona. De este modo, nadie puede entender esos datos, salvo quien los maneja o almacena.

Digital Rights Foundation (Haché, 2021).

TLP:ROJO *No se puede divulgar, está restringido a las personas que participan en él.* Las fuentes pueden utilizar TLP:ROJO cuando la información no puede ser utilizada eficazmente por otras partes y podría tener un impacto en la privacidad, la reputación o las operaciones de una parte si se utiliza de forma indebida. Las personas receptoras no deben compartir información TLP:ROJO con ninguna parte fuera del intercambio, reunión o conversación específica en la que fue expuesta originalmente. En el contexto de una reunión, por ejemplo, la información TLP:ROJO se limita a quienes estaban presentes en la misma. En casi todas las circunstancias, la información clasificada como TLP:ROJO debe intercambiarse verbalmente o de forma presencial.	**TLP:ÁMBAR** *Divulgación limitada, restringida a las organizaciones participantes.* Las fuentes pueden utilizar TLP:ÁMBAR cuando la información requiera apoyo para actuar de forma eficaz pero conlleve riesgos para la privacidad, reputación o las operaciones si se comparte fuera de las organizaciones implicadas. Las personas receptoras únicamente pueden compartir información TLP:ÁMBAR con integrantes de su propia organización y con personas beneficiarias que necesiten conocer la información para protegerse a sí mismas o evitar más daños. Las fuentes tienen derecho a especificar otros límites adicionales para el intercambio de la información que deben ser respetados.
TLP:VERDE *Divulgación limitada, restringida a la comunidad.* Las fuentes pueden utilizar TLP:VERDE cuando la información sea útil para la concienciación de todas las organizaciones participantes, así como con sus pares dentro de una comunidad o sector más amplio. Las personas o entidad receptoras pueden compartir información TLP:VERDE con sus pares y organizaciones asociadas dentro de su sector o comunidad, pero no a través de canales de acceso público. La información de esta categoría puede difundirse ampliamente dentro de una comunidad concreta. La información TLP:VERDE no puede divulgarse fuera de la comunidad.	**TLP:BLANCO** *La divulgación no está limitada* Las fuentes pueden utilizar TLP:BLANCO cuando la información suponga un riesgo mínimo o nulo de uso indebido, dentro de las reglas y procedimientos establecidos para su difusión pública. La información TLP:BLANCO puede ser distribuida sin restricciones, sujeta a controles de derechos de autor.

2. ¿Cómo se gestiona y protege la información?

Es preciso definir cómo se protegen sus comunicaciones y la información que se almacena en su infraestructura, así como durante cuánto tiempo se conserva la información almacenada en la infraestructura y qué sucede en caso de que se produzca una filtración de datos.

3. ¿Qué medidas se establecen para la divulgación de información, especialmente cuando se transmite información relacionada con incidentes a otros equipos o cuando la solicitan las autoridades policiales?

4. ¿Existen aspectos jurídicos que deban tenerse en cuenta en relación con el tratamiento de la información?

5.¿Su política define cómo se debe proteger y utilizar su infraestructura técnica y sus equipos?

Revisa la plantilla de la Política de gestión de la información en la página 83.

Plan de respuesta a incidentes

Los procedimientos de gestión de incidentes descritos en el plan de respuesta a incidentes son una de las medidas clave que deben establecerse, ya que permitirán que todo el mundo entienda qué se espera de cada quién. Describan los distintos tipos de incidentes distinguiendo entre niveles de impacto y establezcan qué pasos debe seguir su equipo. Definan a qué integrantes del equipo hay que dirigirse si surge un incidente. Enumeren las distintas posibilidades para poder elevar o derivar los casos y organícenlas con todo el equipo. Es decir, asegúrense de que las expectativas se gestionan adecuadamente dentro de la organización.

Para contar con un planteamiento documentado y coordinado para responder cuestiones de seguridad digital, el plan de respuesta a incidentes debe incluir los siguientes aspectos:

- Cómo se reciben y asignan los casos.
- Cómo se priorizan los casos.
- El flujo de trabajo de admisión, verificación y escalada de la LASDSC.
- El ciclo de respuesta a incidentes de la LASDSC.
- Cómo se cierran los casos.

Revisa la plantilla del Plan de respuesta a incidentes en la página 77.

Política de verificación

Asegurarse de que una LASDSC apoya a su verdadero público es clave para su reputación, por lo que muchas líneas de ayuda y líneas de atención verifican que las personas solicitantes son realmente quienes dicen ser antes de iniciar el proceso de gestión de incidentes.

Para definir este proceso de verificación, una buena práctica es desarrollar una política de verificación que describa las metas del proceso, así como los pasos que se deben tomar para verificar a la nueva persona beneficiaria, obtener su consentimiento informado sobre el proceso y proteger su privacidad en la medida de lo posible.

Revisa la plantilla de la Política de verificación en la página 89.

Así que, básicamente, empezamos con gente que nos contacta por alguna razón. A menudo porque han recibido un SMS o un correo electrónico extraño, algo así. Luego intentamos recabar información sobre el contexto, investigar el correo electrónico o el SMS que han recibido. Pero primero tenemos que asegurarnos de que son personas defensoras de derechos humanos y eso puede suponer un reto, pues la definición de defensora de DD.HH. de Amnistía Internacional puede ser a veces muy estrecha y depende del equipo del país. Amnistía Internacional trabaja a dos niveles: los equipos del país y los equipos temáticos, así que, por ejemplo, en mi equipo trabajamos en el campo de la tecnología, pero cada vez que trabajamos en un país tenemos que trabajar con el equipo del país. Cuando recibimos una solicitud de ayuda tenemos que comprobar quién es la persona que la realiza y si es defensora de derechos humanos, cosa compleja porque a veces tenemos que preguntar a la gente quién son y luego comprobar con el equipo del país si efectivamente son defensoras de derechos humanos y asegurarnos de que contamos con su aprobación. Y, si es el caso (a menudo con periodistas, por ejemplo, es bastante fácil) hacemos la investigación y tratamos de entender qué pasó.

Etienne Maynier, Amnesty Tech (Entrevista, Diciembre 2021).

Hay distintas buenas prácticas que hemos ido desarrollando a lo largo del tiempo. Empezando por aprender a cuidar de quienes acuden a nuestros proyectos y también del equipo. Sabemos que esto puede resultar agotador, pero tenemos que estar bien para acompañar mejor a otras personas.

Tecnoresistencias (Haché, 2021).

Código de conducta

Un Código de conducta es un documento que establece cómo debe comportarse el personal de la LASDSC cuando se relaciona con las personas beneficiarias. Estos son algunos de los elementos más importantes de un código de conducta eficaz:

- Descripciones específicas de conductas comunes pero inaceptables (comentarios sexistas, etc.).
- Instrucciones para presentar una denuncia con información de contacto.
- Información sobre cómo puede aplicarse.
- Una distinción clara entre el comportamiento inaceptable (que puede ser denunciado siguiendo las instrucciones de denuncia y puede tener consecuencias graves para quien lo ha perpetrado) y las pautas comunitarias, como la resolución general de conflictos.

Los códigos de conducta que carecen de alguno de estos elementos no suelen producir el efecto que se pretende.

Revisa la plantilla del Código de conducta en la página 73.

Otros generadores y plantillas de códigos de conducta:

- **Código de conducta de Berlín** (multilingüe).
- **Generador de códigos de conducta**, basado en el **Contributor Covenant** (multilingüe)
- **Repositorio de Mozilla sobre Diversidad e Inclusión de Código Abierto**, que contiene recursos, modelos y normas para hacer que los proyectos abiertos sean más inclusivos.

Procedimientos operativos estándar para operadores de LASDSC

Es importante que una LASDSC cuente con Procedimientos Operativos Estándar (POE), para definir, por ejemplo, cómo se deben responder las solicitudes, comunicarse con las personas beneficiarias, garantizar la confidencialidad y realizar derivaciones, pero también para asegurar que quienes atiendan las llamadas saben cómo comportarse en situaciones de tensión y afrontar el estrés.

Para saber más

La documentación pública de la línea de ayuda de Access Now incluye una **sección sobre sus procedimientos operativos estándar** (**https://communitydocs.accessnow.org/tag_helpline_procedures.html**).

2

Elabora un plan realista

Una vez definido el marco de trabajo de la LASDSC, es el momento de establecer un plan general que describa cómo llevarlo a cabo, es decir, definir los aspectos materiales. Este plan debe incluir la elaboración de un presupuesto que cubra todas las necesidades operativas: desde el personal, el hardware y el software hasta el alquiler de una oficina si es necesario.

Es fundamental establecer cómo se van a conseguir los recursos para cubrir este presupuesto. ¿Se aceptarán fondos de entidades gubernamentales y privadas? ¿Se financiará a través de un *crowdfunding*? ¿Se intentarán establecer acuerdos con instituciones públicas? La forma en que la LASDSC logre la sostenibilidad económica estará condicionada en gran medida por el entorno institucional definido en el marco de trabajo.

En esta fase es importante definir qué herramientas utilizará la LASDSC, especialmente para el seguimiento de los casos. Hay muchos gestores de tickets distintos, con características, costes y requisitos específicos. Hay que identificar cuál es el que mejor se adapta a las necesidades de la LASDSC. En este capítulo hacemos una comparación de los más populares para que puedan tomar una decisión informada sobre cuál les conviene.

Obviamente, el plan debe incluir una estrategia para proteger al equipo, tanto en el plano digital como en el físico. Hemos incluido algunas directrices básicas en este capítulo, aunque recomendamos encarecidamente contratar a una persona especializada para crear un plan de seguridad riguroso, especialmente si han decidido montar una oficina física y autogestionar su infraestructura.

Por último, es preciso tener una reflexión sobre cómo crear y cuidar al equipo. A la hora de planificar la LASDSC, hay que definir qué competencias básicas debe te-

ner el personal del equipo para prestar los servicios que se quieren ofrecer: ya sea contratando a las personas adecuadas o formando al personal una vez que se hayan incorporado al equipo. También habrá que reflexionar sobre sus funciones y responsabilidades y sobre cómo cuidar su bienestar.

2.1 Crea un presupuesto

El coste de la línea de asistencia dependerá de las decisiones que se hayan tomado, especialmente las que tienen que ver con la estructura organizacional, el tiempo de respuesta y los servicios que se vaya a ofrecer que impliquen costes adicionales (por ejemplo, si se van a ofrecer ayudas para reemplazar equipos robados o pagar la formación del personal).

El presupuesto básico inicial, que servirá para crear la LASDSC y empezar a ofrecer servicios debería cubrir como mínimo:

1. Los sueldos iniciales del personal, a menos que se trate de una línea de atención sostenida completamente por trabajo voluntario.
2. Costes de *hardware* y *software*: dispositivos de trabajo para el personal, equipos de oficina (si va a haber una oficina), licencias de *software*, etc.
3. Coste de los servicios en línea, como el sitio web, una plataforma de intercambio de archivos, un gestor de tickets, etc.
4. Sueldos u honorarios de asesores jurídicos, implementación de servicios, etc.
5. Formación del personal.
6. Alquiler de la oficina (en caso de que se decida trabajar desde una oficina).

Se puede elaborar un presupuesto de mínimos, que incluya lo imprescindible para que sea viable desde el punto de vista operativo y un presupuesto de máximos, en caso de que se consigan todos los recursos necesarios.

Este presupuesto debe revisarse una vez finalizada la fase de diseño, con todas las decisiones operativas tomadas.

Para saber más

Lee más sobre buenas prácticas para crear un presupuesto en ENISA (2020). "High-level roadmap and budget". ENISA, How to set up CSIRT and SOC - Good Practice Guide (pp. 16-18). **https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc**.

2.2 Decide cómo se financiará tu LASD

Para garantizar que la LASDSC pueda trabajar a largo plazo y convertirse en un punto de referencia para sus beneficiarias, será preciso desarrollar un modelo de financiación fiable que cubra los costes.

Si la LASDSC forma parte de una organización más grande, probablemente pueda recurrir a la organización anfitriona para estudiar la forma de cubrir los costes. Pero si es una organización independiente, conviene pensar en las siguientes cuestiones:

* ¿De dónde procederán los fondos? ¿Se solicitarán subvenciones, se pedirán donaciones, la financiará un consorcio de organizaciones o se cubrirán los gastos ofreciendo algunos servicios de pago?

- ¿Habrá que buscar varias fuentes de financiación o bastará con una para garantizar el funcionamiento a largo plazo?
- ¿Cuán seguras son sus fuentes de financiación?
- ¿La fuente de financiación es estable o terminará en algún momento?
- ¿Se limitará a buscar recursos financieros o tratará de establecer relaciones de colaboración con organizaciones e instituciones asociadas?

Política de financiación

Algunas organizaciones también tienen una política de financiación para determinar si una nueva fuente de financiación es coherente con su misión y objetivos. Por ejemplo, algunos grupos deciden recibir únicamente donaciones para seguir siendo completamente independientes, mientras que otros no aceptan fondos que puedan influir en sus prioridades.

Algunos ejemplos de políticas de financiación de miembros de CiviCERT:

Access Now

La mayor parte del apoyo que recibimos procede de fundaciones y agencias de desarrollo, el resto es de empresas, tribunales, particulares y organizaciones de la sociedad civil. Para garantizar la independencia y la integridad de nuestra organización, aceptamos apoyo sujeto a las siguientes condiciones no negociables:

- Access Now no acepta financiación que ponga en riesgo a su personal, a sus socias, a las comunidades que apoya o a su misión.
- Access Now no acepta financiación que ponga en peligro la relación con sus socias, partes interesadas o comunidades y redes que apoya.
- Access Now no acepta financiación que comprometa su independencia organizativa, como relaciones con fondos que puedan influir en sus prioridades, posturas políticas, iniciativas de incidencia política, regiones de actuación o acción directa.
- Access Now no acepta financiación que plantee un riesgo para su reputación en general o en lo que respecta a áreas de trabajo específicas.

Amnistía Internacional

La inmensa mayoría de nuestros ingresos procede de las donaciones de personas de todo el mundo. Estas donaciones personales y no afiliadas permiten que Amnistía Internacional (AI) mantenga una independencia plena de todo gobierno, ideología política, interés económico o religión. Ni solicitamos ni aceptamos de gobiernos o partidos políticos fondos para nuestra actividad de investigación en derechos humanos y solo aceptamos el apoyo de empresas que han sido objeto de escrutinio previo. Una recaudación de fondos ética, principalmente de donaciones de personas particulares, es lo que nos permite mantenernos firmes e inquebrantables en nuestra defensa de derechos humanos universales e indivisibles. El movimiento global de Amnistía está compuesto por una red de Secciones nacionales y el Secretariado Internacional.

Los retos que hemos detectado hasta ahora están relacionados con la sostenibilidad, porque la línea de ayuda es un proyecto financiado. ¿Y qué pasa si no hay financiación? ¿Cómo la mantenemos? ¿Cómo la gestionamos? Para ello, hemos creado algunos recursos para que la gente pueda acceder a ayuda. Uno de ellos es un portal de juristas y profesionales que pueden ofrecer servicios jurídicos gratuitos a mujeres que sufren acoso en línea, por ejemplo.

Digital Rights Foundation (Haché, 2021).

Para saber más

Política de financiación de Access Now (**https://www.accessnow.org/financials/**).

Política de financiación de Amnistía Internacional (**https://www.amnesty.org/en/about-us/how-were-run/finances-and-pay**).

2.3 Seguridad física del personal y las oficinas

Tanto si decides montar una oficina física como si no, debes elaborar un plan para proteger al personal, a las personas voluntarias, la oficina y la infraestructura de posibles ataques físicos.

A la hora de plantear la seguridad física de la oficina, se debe tener en cuenta, por ejemplo:

- La protección del *hardware* que contiene información sensible: ordenadores, discos duros externos, servidores, etc.
- Asegurarse de que nadie accede a la oficina sin permiso. Por ejemplo, instalando una cámara de seguridad en la entrada de la oficina o concienciando al equipo sobre quién puede acceder a su lugar de trabajo y quién no.
- Proteger las impresoras y los documentos impresos de accesos no autorizados y destruir los documentos impresos que ya no se utilicen.
- Asegurar los *routers* y la infraestructura de comunicaciones.
- Recordar al equipo que nunca debe dejar sus ordenadores sin supervisión. Y si lo hacen, deben dejarlo siempre bloqueado.

Para saber más

Pueden encontrar recomendaciones de seguridad física para su oficina o para las personas que trabajen de forma voluntaria desde su casa en Access Now Helpline Security Policy Templates. **https://gitlab.com/AccessNowHelpline/helpline_documentation_resources/-/tree/master/templates/organisational_Security_Policies-Templates.**

Higson Smith, Craig, Ó Cluanaigh, Daniel, Ravi, Ali G., Steudtner, Peter (2016). *Holistic Security - A Strategy Manual for Human Rights Defenders*. Tactical Technology Collective. **https://holistic-security.tacticaltech.org.**

Eguren, Enrique, y Caraj, Marie (eds.) (2009). *Nuevo manual de protección para los defensores de derechos humanos*. Protection International. **https://www.protectioninternational.org/wp-content/uploads/2012/04/Nuevo_Manual_Proteccion.pdf.**

Tsunga, Arnold (ed.) (2007). *Protection Handbook for Human Rights Defenders*. Front Line, The International Foundation for the Protection of Human Rights Defenders. **https://www.frontlinedefenders.org/fr/file/1671/download?token=XHaqzSCK.**

2.4 Seguridad de la red

Si el equipo trabaja en una oficina, debe tener una red exclusiva para conectarse a Internet, así como a las impresoras, los servidores físicos, etc. Si se quiere dejar que las visitas utilicen el Wi-Fi, es preciso crear una red separada para ello.

Si es posible, valoren la posibilidad de contratar a una persona administradora de sistemas para que gestione la red de su oficina, así como su propia infraestructura, si han decidido autogestionar el alojamiento de sus herramientas y plataformas en línea.

2.5 Infraestructura y herramientas

En teoría, se puede crear una LASDSC con tan solo un ordenador por integrante del equipo y una plataforma de colaboración segura, como una instancia autoalojada de NextCloud, Gitlab o Discourse, para compartir información entre el equipo, organizar las tareas, hacer un seguimiento de los contactos, etc. Incluso se puede recurrir a un **proveedor de servicios afín** para que aloje dicha plataforma en un lugar compatible con el modelo de amenazas de la LASDSC.

Si el presupuesto lo permite, al planificar su línea de atención deben plantearse el uso de herramientas creadas explícitamente para la gestión de incidentes, la identificación de indicadores de compromiso, el intercambio de información y el análisis de programas maliciosos.

Muchas LASDSC utilizan las siguientes herramientas para gestionar y analizar incidentes:

- Un gestor de tickets para gestionar los casos y solicitudes de apoyo (véase más abajo la sección *Sistemas de gestión de tickets*).
- Una instancia autogestionada o federada de MISP para compartir, almacenar y correlacionar indicadores de compromiso (**https://www.misp-project.org/**).
- Un sistema de análisis de *software* malicioso como Cuckoo Sandbox (**https://cuckoosandbox.org/**).
- A veces, un CRM para la gestión de contactos como CiviCRM **(https://civicrm.org).**

En general, a la hora de elegir una herramienta o servicio, lo mejor es seguir estas pautas:

- El *software* debe ser libre y de código abierto.
- Lo ideal es que el alojamiento sea autogestionado o que sea brindado por una entidad de confianza.
- Si el servicio lo aloja un tercero, debe estar cifrado de extremo a extremo (E2E), auditado y ofrecer un buen nivel de seguridad, por ejemplo, con autentificación de doble factor (2FA).

Sistemas de gestión de tickets

Desde el momento en que se recibe una solicitud de ayuda, la persona encargada del caso debe empezar a anotar todos los detalles relacionados con la persona beneficiaria, el incidente y las medidas que se han tomado para gestionarlo. El registro de todas las comunicaciones con la beneficiaria, así como de todos los pasos que se han dado para detectar y abordar el incidente, puede facilitar la colaboración con el resto del equipo y la derivación a otras organizaciones, ayudar a mejorar los procedimientos de gestión de incidentes y proporcionar pruebas que pueden ser útiles en un tribunal.

Los casos se pueden documentar de muchas formas, incluso en documentos de texto o en papel, pero el uso de un gestor de tickets simplificará esta tarea. Este tipo de herramienta permite registrar y organizar cada comunicación y detalle de forma sistemática, facilitando el seguimiento de cada solicitud de apoyo, así como de las personas beneficiarias y de las terceras partes relevantes. Además permite la revisión de casos anteriores en aras de una garantía de calidad y de poder generar

estadísticas... por poner algunos ejemplos de funciones importantes que pueden ser útiles para el trabajo de una LASDSC.

Debido a que las comunicaciones pasan por el gestor de tickets y se almacenan ahí, una de las cuestiones básicas que se debe valorar a la hora de elegir la herramienta que se va a utilizar para el seguimiento de las solicitudes, es la posibilidad de proteger las comunicaciones y la información de los incidentes. Por ello, es recomendable elegir un sistema que sea compatible con herramientas de cifrado, como correos electrónicos cifrados con GPG o aplicaciones de mensajería segura como Signal.

Además, un gestor de tickets debe permitir el registro de la siguiente información:

- Nombre y dirección de correo electrónico de la persona beneficiaria.
- Estado de verificación de la beneficiaria (verificado, no verificado, rechazado).
- Tipo de colectivo al que pertenece.
- Estado actual del incidente (nuevo, abierto, cerrado, etc.)
- Urgencia y prioridad del incidente.
- Un resumen del incidente.
- Tipo de servicio solicitado para resolver el incidente.
- Todas las comunicaciones con la persona beneficiaria.
- Pruebas recogidas durante la investigación del incidente.
- Indicadores relacionados con el incidente.
- Otros casos relacionados con este incidente.
- Medidas adoptadas para este incidente.
- Información de contacto de otras partes implicadas (por ejemplo, intermediarias, empresas a las que se ha recurrido para una derivación, socias que están ayudando a gestionar el caso, etc.)
- Todas las comunicaciones con otras partes implicadas.
- Comentarios de las personas que han gestionado el incidente.
- Próximos pasos.

A continuación, presentamos una visión general de los gestores de tickets más utilizados en el ámbito del apoyo a la seguridad digital para la sociedad civil.

Zammad y CDR Link

Zammad es un sistema de gestión de tickets de código abierto, con interfaz web y funciones para gestionar las comunicaciones a través de varios canales como vía telefónica, Facebook, Twitter, chat y correo electrónico, entre otros.

Ante las necesidades específicas de la sociedad civil y de las personas defensoras de los derechos humanos, el **Center for Digital Resilience** (**https://digiresilience.org/**) ha desarrollado **CDR Link** (**https://docs.digiresilience.org/link/about/**), un gestor de tickets centrado en la privacidad y la seguridad y basado en Zammad que cuenta con *plug-ins* de mensajería personalizados para Signal, WhatsApp y GPG, para proteger las comunicaciones. CDR Link requiere cuentas de Google para iniciar sesión y está alojado en Amazon Web Services (AWS).

Zammad también se puede integrar con NextCloud (a partir de la versión 20): la **app de integración de Zammad para NextCloud** (**https://apps.nextcloud.com/apps/integration_zammad**) ofrece un *widget* de panel con una visión general de los tickets de Zammad, soporte para buscar tickets de Zammad utilizando la búsqueda unificada de NextCloud y notificaciones sobre las actualizaciones de estado de los tickets.

Request Tracker

Request Tracker (**https://bestpractical.com/request-tracker**), o RT, es una plataforma de flujos de trabajo y seguimiento de problemas de código abierto desarrollada

y apoyada por **Best Practical Solutions** (**https://bestpractical.com/**).

RT puede alojarse en un servidor propio, pero también hay opciones de alojamiento gestionado o en la nube con AWS. Puede integrarse con cifrado PGP y es uno de los gestores de tickets más utilizados por los equipos de apoyo a emergencias informáticas. Entre ellos, cabe destacar cómo las soluciones documentadas durante la gestión de un incidente pueden rápidamente **convertirse en documentación de procedimiento** (**https://rt-wiki.bestpractical.com/wiki/Articles#Extracting_an_Article**) dentro de la propia RT.

Freescout

Freescout (**https://freescout.net**) es un gestor de tickets libre y de código abierto que puede instalarse fácilmente incluso en un alojamiento compartido. Puede alojarse en un servidor propio, pero **también está disponible el alojamiento gestionado** (**https://github.com/freescout-helpdesk/freescout/wiki/Cloud-Hosted-FreeScout**).

Freescout ofrece **módulos de pago** que pueden ampliar sus funcionalidades, incluida la integración con **PGP** (solo firma y cifrado (**https://freescout.net/module/mail-signing**), **WhatsApp** (**https://freescout.net/module/whatsapp**), **Telegram** (**https://freescout.net/module/telegram-integration**) y **Twitter** (**https://freescout.net/module/twitter/**)

Trac

Trac (**https://trac.edgewall.org**) es un sistema de gestión de proyectos y seguimiento de errores de código abierto, interfaz web, que **puede utilizarse para el seguimiento de tareas, problemas e incidentes** (**https://trac.edgewall.org/wiki/TracTickets**)y a veces lo utilizan las líneas de atención para gestionar sus casos. Puede alojarse en un servidor propio, pero **también está disponible el alojamiento gestionado** (**https://trac.edgewall.org/wiki/CommercialServices**)

GLPI

GLPI (**https://glpi-project.org**) -acrónimo francés para *Gestionnaire Libre de Parc Informatique* o "Gestor Libre de Equipos Informáticos"- es un sistema de seguimiento y servicio de atención al cliente libre y de código abierto. Puede **alojarse en servidor propio** (**https://glpi-install.readthedocs.io/en/latest/**) pero **también está disponible el alojamiento gestionado** (**https://www.glpi-network.cloud/**).

Primero y GBVIMS

Primero (**https://www.primero.org/**) es una plataforma de *software* de código abierto alojado en servidores propios para el seguimiento de incidentes y la gestión de casos de servicios sociales, incluida la protección de la infancia y la violencia de género.

Basado en Primero, el *Gender-Based Violence Information Management System* (GBVIMS - **https://www.gbvims.com**) es un sistema de gestión de datos que permite a quienes prestan servicios a supervivientes de violencia de género recopilar, almacenar, analizar y compartir de forma eficaz y segura los datos relacionados con los incidentes denunciados.

Otros

Hay muchas herramientas útiles que pueden integrar los tickets del proceso de gestión en su flujo de trabajo actual. Como hemos mencionado antes, si su organización ya está utilizando NextCloud hay un *plug-in* específico para la integración de Zammad. Si utiliza Discourse puede añadir un gestor de tickets usando los *plug-ins* **tickets** (**https://meta.discourse.org/t/tickets-plugin/97914**) y **assign** (**https://meta.discourse.org/t/discourse-assign/58044**).

Una herramienta de gestión de tickets estándar puede ser excesiva para organizaciones pequeñas. Pero existen muchas herramientas de gestión de proyectos que pueden cumplir perfectamente la función y que son mucho más sencillas de utilizar. Por ejemplo, **NextCloud Deck** (**https://apps.nextcloud.com/apps/deck**) es una forma sencilla y fácil de gestionar tickets. Su simplicidad es una gran ventaja para organizaciones pequeñas. En NextCloud Desk cada ticket es una tarea, una tarea lleva una descripción, se califica con etiquetas, tiene una fecha de

inicio y de vencimiento y se puede desplazar de una columna a otra para replicar el flujo de trabajo de los tickets.

2.6. Gestión del equipo

Toda LASDSC tiene que contar con un equipo de personas que tengan una serie de habilidades específicas para responder a las solicitudes de apoyo de forma ágil y acertada. El tamaño y experiencia del equipo dependerá del diseño organizacional y de la situación financiera, así como de la capacidad de crear, coordinar y cuidar el desarrollo profesional y el bienestar del equipo.

Habilidades deseadas

Una LASDSC debe definir el conjunto de habilidades necesarias para cumplir su misión. Puesto que la tarea de la línea de atención es responder a solicitudes de seguridad digital, hay una serie de habilidades básicas que el equipo debe cumplir.

La siguiente es una lista orientativa de las habilidades técnicas e interpersonales que debe reunir el personal de una LASDSC. Si el equipo no posee alguna de las habilidades necesarias, deberá identificar a una tercera parte a la que externalizar la tarea para la que se necesita esa habilidad.

Conjunto de habilidades técnicas

- Capacidad para administrar sistemas GNU/Linux-UNIX.
- Capacidad para administrar servidores web.
- Familiaridad con los sistemas operativos más comunes: Windows, GNU/Linux, macOS, Android e iOS.
- Capacidad para trabajar con al menos una herramienta de análisis de red como Wireshark, tcpdump, Zeek, Snort, etc.
- Conocimiento práctico de toda la gama de protocolos de red OSI o TCP/IP, incluidos los principales protocolos como IP, protocolo de mensajes de control de Internet (ICMP, por sus siglas en inglés), TCP, protocolo de datagramas de usuario (UDP, por sus siglas en inglés), protocolo simple de transferencia de correo (SMTP, por sus siglas en inglés), protocolo de oficina de correos 3 (POP3, por sus siglas en inglés), protocolo de transferencia de hipertexto (HTTP, por sus siglas en inglés), protocolo de transferencia de archivos (FTP, por sus siglas en inglés) y SSH.
- Conocimiento práctico de algoritmos y protocolos de criptografía populares como Advanced Encryption Standard (AES), Rivest, Shamir y Adleman (RSA), Message-Digest Algorithm (5) (MD5), Secure Hash Algorithm (SHA), Kerberos, Secure Socket Layer/ Transport Layer Security (SSL/TLS) y Diffie-Hellman.
- Capacidad para realizar evaluaciones de vulnerabilidad y trabajar con herramientas de pruebas penetración como Kali Linux, Metasploit, etc.
- Conocimiento de scripts con lenguajes y herramientas como Python, bash, awk, sed, grep, etc.
- Familiaridad con las técnicas y tácticas de los ataques.
- Conocimiento sólido de la gestión de personas usuarias finales de plataformas de redes sociales como Facebook, Instagram, Twitter, Youtube, etc.
- Para quienes trabajen con ingeniería inversa de *software* malicioso, conocimientos de código de montaje en Intel x86 y manejo de diversas utilidades que ayudan al análisis de *software* malicioso, como SysInternals, así como suites de herramientas utilizadas para descompilar y analizar *software* malicioso como IDA y Ghidra.

Sin duda, las personas con formación en informática y estudios de seguridad informática estarán seguramente mejor preparadas para dominar estas habilidades. Sin embargo, también hay quienes sienten pasión por estos campos y que podrían adquirir y demostrar estos conocimientos con rapidez. A la hora de contratar, conviene evaluar la formación, la experiencia y el nivel de entusiasmo para seleccionar a una persona adecuada que se incorpore al equipo.

Por lo general, durante la creación de una línea de atención, no siempre se logra contar con estos conocimientos con la rapidez que se desea. Por lo tanto, la dirección debe centrarse en identificar las capacidades que son absolutamente necesarias para cumplir la misión de la LASDSC y, a continuación, cubrir las carencias formando al equipo, realizando una campaña de contratación específica o subcontratando ciertas tareas a otros equipos.

Habilidades interpersonales

Las habilidades interpersonales son tan importantes como las técnicas, sobre todo para las personas que estarán en contacto directo con las beneficiarias.

- Buena comunicación escrita y oral en inglés, para coordinarse con otras entidades asociadas y en las lenguas locales de la región en la que centrarán su trabajo.
- Capacidad para trabajar en entornos con un ritmo de trabajo intenso y con mucho estrés.
- Gran capacidad para trabajar en equipo.
- Capacidad para impartir formación práctica y compartir conocimientos con el resto del equipo.
- Capacidad de iniciativa propia y de gestión del tiempo.
- Un profundo sentido de integridad y de identificación con la misión de la LASDSC.
- Amplia comprensión de la cultura y experiencia en la región en la que se trabaja.
- Comprensión profunda del contexto político de la LASDSC.
- Sensibilidad interseccional en el trabajo con las personas beneficiarias.

Roles y responsabilidades

Una LASDSC conlleva muchas funciones, cada una de ellas con distintas responsabilidades. Tenerlas en cuenta puede ayudar a diseñar la estructura del equipo y a identificar qué puestos necesitan –o pueden– cubrir en función de su marco de trabajo y presupuesto.

- **El personal de primera línea que gestiona las incidencias**. Al ser quienes estarán en contacto directo con las personas beneficiarias y coordinarán las múltiples tareas que propiciarán una respuesta satisfactoria, son el núcleo del equipo. Además de las imprescindibles habilidades de comunicación para entender las necesidades de las personas beneficiarias y transmitirles las instrucciones, este personal de primera línea debe ser capaz de seguir las comunicaciones internas entre el equipo, identificar las lagunas en la documentación y manejar los diferentes recursos disponibles para llevar a cabo la gestión de incidentes, como son el *software* (gestores de tickets, *software* para comunicaciones seguras y herramientas para realizar el triaje) y los recursos humanos, ya sean internos (analistas de segundo nivel) o externos (analistas externos, proveedores de servicios y otras personas o entidades asociadas).

- **Responsable de los turnos**. Su función es coordinar a las personas que atienden las incidencias a lo largo de un turno. En las líneas de atención pequeñas puede ser la propia dirección.
- **Analistas de segundo nivel**. Su función es proporcionar apoyo técnico a las personas que gestionan los incidentes cuando se trata de casos difíciles.
- **Responsable de operaciones**. Gestionan la economía del equipo y sus necesidades en términos de *hardware*, ubicación, logística, etc. Estas tareas podrían ser asumidas por la dirección en LASDSC pequeñas, luego se puede contratar a personal para esta función o externalizar.
- **Coordinación de documentación**. La función de la persona que coordina la documentación es gestionar la base de conocimientos de la LASDSC. Debe encargarse de mantener la documentación existente y ayudar a identificar las lagunas y oportunidades para editar y crear la documentación necesaria para la línea de atención y, especialmente, para que quienes gestionan las incidencias en primera línea puedan realizar su tarea.
- **Administración de sistema**. Su función es crear y mantener la infraestructura que la línea de atención utilizará en su funcionamiento cotidiano. Esta tarea puede externalizarse o, en líneas de atención pequeñas, lo puede asumir la dirección o las personas responsables de incidencias.
- **Asesora jurídica**.Esta persona ayudará a evaluar la seguridad jurídica de las distintas intervenciones que realice la línea de atención y se asegurará de que sus políticas cumplen el marco jurídico vigente (protección de datos personales, por ejemplo).
- **Asesora psicosocial**. Quien brinde asesoría psicosocial puede formar a las gestoras de incidentes de la LASDSC para que respondan a las solicitudes de apoyo sin revictimizar y para que adquieran las habilidades necesarias para atender a las personas con trastornos emocionales.
- **Externalización de tareas**.A la hora de externalizar cualquier tarea, se debe hacer siempre con un equipo o persona con la que existe un nivel de confianza muy alto. Teniendo en cuenta las características de una línea de atención que trabaja con la sociedad civil y con personas defensoras de los derechos humanos, los contratos y acuerdos de confidencialidad son sin duda necesarios, pero no suficientes para garantizar el nivel de seguridad que necesita el público de una LASDSC.

Entre 2019 y 2021, DDP puso en marcha un proyecto para desarrollar las capacidades de formadoras que pudieran brindar un apoyo sostenible y holístico en materia de seguridad a personas defensoras de derechos humanos en el sudeste asiático, América Latina y África. Este proceso se desarrolló en dos fases: por un lado, el objetivo era fortalecer las capacidades de las personas que brindan protección en general; por otro, se pretendía involucrar directamente a algunas de las personas participantes para llevar a cabo procesos de acompañamiento. Una vez finalizado, DDP lanzó una convocatoria para las participantes que deseasen formar parte del equipo de Facilitadoras de Protección Digital de DDP. El proyecto fue un pilar del proyecto más amplio de DDP de descentralizar y reforzar el grado de integración de su equipo en los movimientos de derechos humanos del Sur Global.

Daniel Ó Cluanaigh, Digital Defenders Partnership.

Crea tu equipo

La contratación de personal para la línea de atención es un proceso decisivo para el éxito del proyecto. Además de las competencias técnicas e interpersonales, deben compartir los valores del equipo y comprometerse genuinamente a prestar apoyo a su público. A la hora de buscar nuevo personal para el equipo, es importante tener en cuenta los siguientes aspectos:

- La confianza de las comunidades a las que se apoya es más importante que las competencias puramente técnicas. La sintonía con los valores y el compromiso con la misión del equipo deben figurar entre los principales requisitos para todos los puestos.
- El desarrollo de las competencias técnicas siempre es posible, siempre y cuando se disponga de tiempo y de recursos para apoyar el proceso de formación.
- Los procesos de incorporación marcan una gran diferencia en cuanto a la rapidez con la que el personal de una línea de atención puede empezar a prestar asistencia de calidad. Siempre que sea posible, redacten unas directrices sobre todos los temas que cubre la línea y sigan una metodología de mentoría.

Se puede optar por contratar a una persona y luego formarla en las competencias que necesita para trabajar en la LASDSC, o se puede lanzar una campaña de capacitación comunitaria para formar a activistas que luego colaboren en la línea de atención. Si deciden adoptar este planteamiento, incorporen un **enfoque holístico** (ver por ejemplo **https://holistic-security.tacticaltech.org/trainers-manual.html**) a sus sesiones de formación y un marco como el modelo ADIDS (acrónimo en inglés para Actividad-Discusión-*Input*-Profundización-Síntesis).

Más información sobre el modelo ADIDS en los siguientes recursos:

Cómo abordar el aprendizaje en adultos (en inglés **https://level-up.cc/before-an-event/levelups-approach-to-adult-learning/**) Level Up

Cómo diseñar sesiones usando ADIDS (en inglés **https://level-up.cc/before-an-event/preparing-sessions-using-adids/**) Level Up

Módulo de formación de formadores sobre aprendizaje en adultos y ADIDS (en inglés **https://www.fabriders.net/tot-adids/**) Fabriders

Formación y desarrollo profesional

Para desarrollar los conocimientos y habilidades del equipo de la línea de atención, deben ofrecerse distintas posibilidades, ya que una única estrategia de trabajo para todo el personal puede no ser posible o adecuada.

Cada integrante del equipo debe trabajar conjuntamente con sus responsables directas para elaborar planes de formación y desarrollo. Estos deben revisarse de forma periódica y se deben registrar los progresos durante las intervenciones o las revisiones de rendimiento.

Los planes de desarrollo personales pueden variar: desde formación en línea, adquisición de libros y revistas o asistencia a formación presencial.

Además de estos planes personales, la organización de las líneas de atención debe compartir recursos a nivel interno de forma continua, en especial sobre temas que son relevantes para todo el equipo, como cuestiones técnicas sobre seguridad digital y otras, entre ellas el autocuidado, el apoyo psicológico y la seguridad física.

Proporcionar materiales y fomentar el autoaprendizaje

Las responsables de las líneas de atención deben hacer circular recursos dentro del equipo para ampliar sus conocimientos técnicos sobre diferentes temas relacionados con la seguridad. Esto debe plantearse como una invitación abierta, para que el equipo consulte y utilice esos recursos, no se debe hacer un control posterior para comprobar si se están aplicando los conocimientos. El objetivo principal es proporcionar información que se ajuste a sus intereses y fomentar una cultura de autoaprendizaje.

Además de los recursos en línea, también se pueden facilitar libros y revistas que puedan ser útiles para el trabajo de la línea de atención. Las revistas y los libros se proporcionarán a petición del equipo o cuando la dirección de la línea de atención considere que pueden tener un impacto positivo en el desarrollo de este.

Formación externa

Cuando sea apropiado y siempre que los recursos lo permitan, la dirección de la línea de atención debe apoyar a las personas del equipo para que participen en cursos de formación técnica, de acuerdo con sus planes personales de formación.

Conferencias

Es importante tratar de facilitar que el personal tenga al menos una oportunidad al año para asistir a un evento relacionado con la línea de atención.

Conviene conocer las conferencias futuras y tratar de asistir a eventos que sean relevantes para el trabajo con grupos de la sociedad civil y otras organizaciones y personas que prestan estos servicios de seguridad digital.

Una de las mejores formas de localizar conferencias y eventos relevantes es preguntar a las personas beneficiarias a qué eventos acuden o les gustaría que asistiera el personal del equipo.

Ejemplos de conferencias que pueden ser relevantes para una línea de atención orientada a la sociedad civil

Evento	Frecuencia	Página web	Contenido
Bread&Net	*Anual*	https://www.breadandnet.org/en/	Desconferencia anual que promueve y defiende los derechos digitales en países de lengua árabe.
Chaos Communications Congress	*Anual*	https://events.ccc.de/	Adquisición de conocimientos técnicos, conocer a nuevas personas beneficiarias o socias.
Dublin Platform	*Cada dos años*	https://www.frontlinedefenders.org/en/programme/dublin-platform	Reunión bienal de personas defensoras de derechos humanos.
FIFAfrica	*Anual*	https://cipesa.org/fifafrica/	Foro sobre la libertad de Internet en África.
Encuentros globales y regionales de la Rapid Response Network	*Anual*	https://rarenet.org	Encuentro entre miembros de Rapid Response Network.
Global Internet Governance Forum	*Anual*	https://www.intgovforum.org	Plataforma global de múltiples partes interesadas que facilita el debate sobre cuestiones de política pública relacionadas con Internet.

ILGA World (& conferencias regionales)	*Anual*	https://ilga.org/es/conferencias-mundiales	Encuentros mundiales y regionales de activistas LGTBQIA+.
MozFest	*Anual*	https://www.mozillafestival.org/	Conferencia sobre tecnología organizada por Mozilla.
Regional Internet Governance Forums	*Anual*	https://www.intgovforum.org/multilingual/content/regional-igf-initiatives	Conferencias regionales para facilitar el debate sobre cuestiones de política pública relacionadas con Internet.
Encuentro Global de CiviCERT	*Anual*	https://civicert.org	Encuentro de integrantes del CiviCERT
RightsCon	*Anual*	https://rightscon.org	Encuentro mundial sobre derechos digitales organizado por Access Now.
Stockholm Internet Forum	*Anual*	https://stockholminternetforum.se/	Foro internacional que promueve una Internet libre, abierta y segura como motor de desarrollo mundial.

Eventos de Trusted Introducer

CiviCERT (**https://civicert.org**) es un CERT acreditado por **Trusted Introducer** (**https://www.trusted-introducer.org/**)y como tal, los miembros de CiviCERT pueden participar en encuentros y sesiones de formación para equipos de seguridad y respuesta a incidentes. Aquí **https://www.trusted-introducer.org/events.html** puedes encontrar los próximos eventos.

Plataformas web

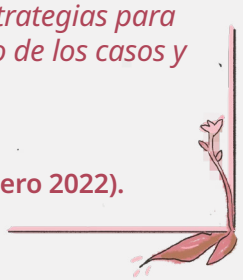
También se puede ofrecer al equipo acceso a cursos en plataformas en línea. Estos suelen ser más baratos que los presenciales y permiten que el equipo los realice a su ritmo y en función de la carga de trabajo.

Algunas de estas plataformas podrían ser:

* **Pluralsight: https://pluralsight.com/**
* **Udemy: https://www.udemy.com/**
* **Cybrary: https://www.cybrary.it/**
* **Coursera: https://www.coursera.org/**

Damos prioridad a una carga de trabajo equilibrada entre las personas que atienden los casos. Rotamos la recepción de nuevos casos cada semana para distribuirlos de manera equitativa. Por otro lado, es habitual que haya semanas en las que el número de casos aumenta y cuando esto ocurre y supera las posibilidades de las personas que acompañan, buscamos estrategias para reorganizar el seguimiento de los casos y rebajar la carga.

Luchadoras (Entrevista, Enero 2022).



Sesiones de intercambio

Es importante animar a las personas del equipo que han adquirido conocimientos que puedan ser útiles para las demás (ya sea en el desempeño de su trabajo o tras realizar una formación) a que lo documenten mediante artículos y a que ofrezcan sesiones de intercambio de conocimientos al resto del equipo. Si las sesiones de intercambio de conocimientos se graban, servirán de apoyo para el aprendizaje del resto del equipo y de las nuevas contrataciones.

Políticas de cuidados

Quienes atienden las incidencias en una línea de atención gestionan un amplio conjunto de situaciones estresantes que pueden afectarles. Cuidar el bienestar psicoemocional del equipo evita el agotamiento, el desgaste y aumenta la calidad de la atención prestada.

Es tan importante cuidar el bienestar del equipo como el de las personas beneficiarias. Por ello, conviene asignar todo tipo de recursos (tiempo, recursos humanos, dinero, etc.) para desarrollar un enfoque de cuidado psicoemocional en sus estrategias de gestión de equipos.

No existe una forma universal de lograrlo. Depende de las necesidades del personal y de la noción que tengan de los cuidados. Algunas estrategias de cuidado para garantizar el bienestar del equipo pueden ser:

- Aunque la línea de atención sea voluntaria, ofrezcan buenas condiciones de trabajo: complementos, prestaciones, vacaciones, etc.
- Destinen un porcentaje del presupuesto (hasta el 30%) a actividades de cuidado colectivo.
- Planifiquen turnos cortos para que las personas que atienden las incidencias puedan concentrarse y prestar una mejor atención.
- Establezcan reuniones semanales para analizar los casos y aportar una visión colectiva.
- Incluyan la figura de asesora de salud mental para apoyar a las personas que gestionan los incidentes y evitar el agotamiento o el estrés.
- Al inicio de cada turno de gestión de incidentes, se debe establecer una instancia de control para evaluar si la gestora se encuentra en un buen momento para brindar apoyo. Si no lo está, puede sustituirla otra que no tenga asignado un turno específico.
- Establezcan una serie de parámetros para saber cuándo una llamada es demasiado comprometida y requiere la rápida derivación a una responsable. Por ejemplo, si la persona que llama corre un riesgo inminente. Es preciso tener en cuenta estos pasos para proteger a la gestora de incidentes de un estrés excesivo.
- Planifiquen una reunión anual de todo el equipo para debatir los retos, identificar los aprendizajes y ajustar las estrategias de cuidado de la línea de atención.

Pueden redactar una política de cuidados que establezca todas estas estrategias y a la que el equipo y la dirección puedan recurrir para crear un entorno de trabajo saludable. Asimismo, se debe prever un enfoque psicoemocional a la hora de redactar el procedimiento de gestión de incidentes (garantizando un triaje y una asignación de casos equilibrada entre el equipo), un código de conducta, un mecanismo de quejas internas y otras políticas.

Proceso de gestión de incidentes

Una parte fundamental del trabajo de muchas LASDSC es la respuesta a incidentes. Toda línea de atención debe clarificar de antemano los pasos y recursos necesarios para atender una solicitud de apoyo.

El proceso de gestión de incidentes es un proceso continuo y generalmente consta de las siguientes cuatro etapas:

Fase 1: Preparación.

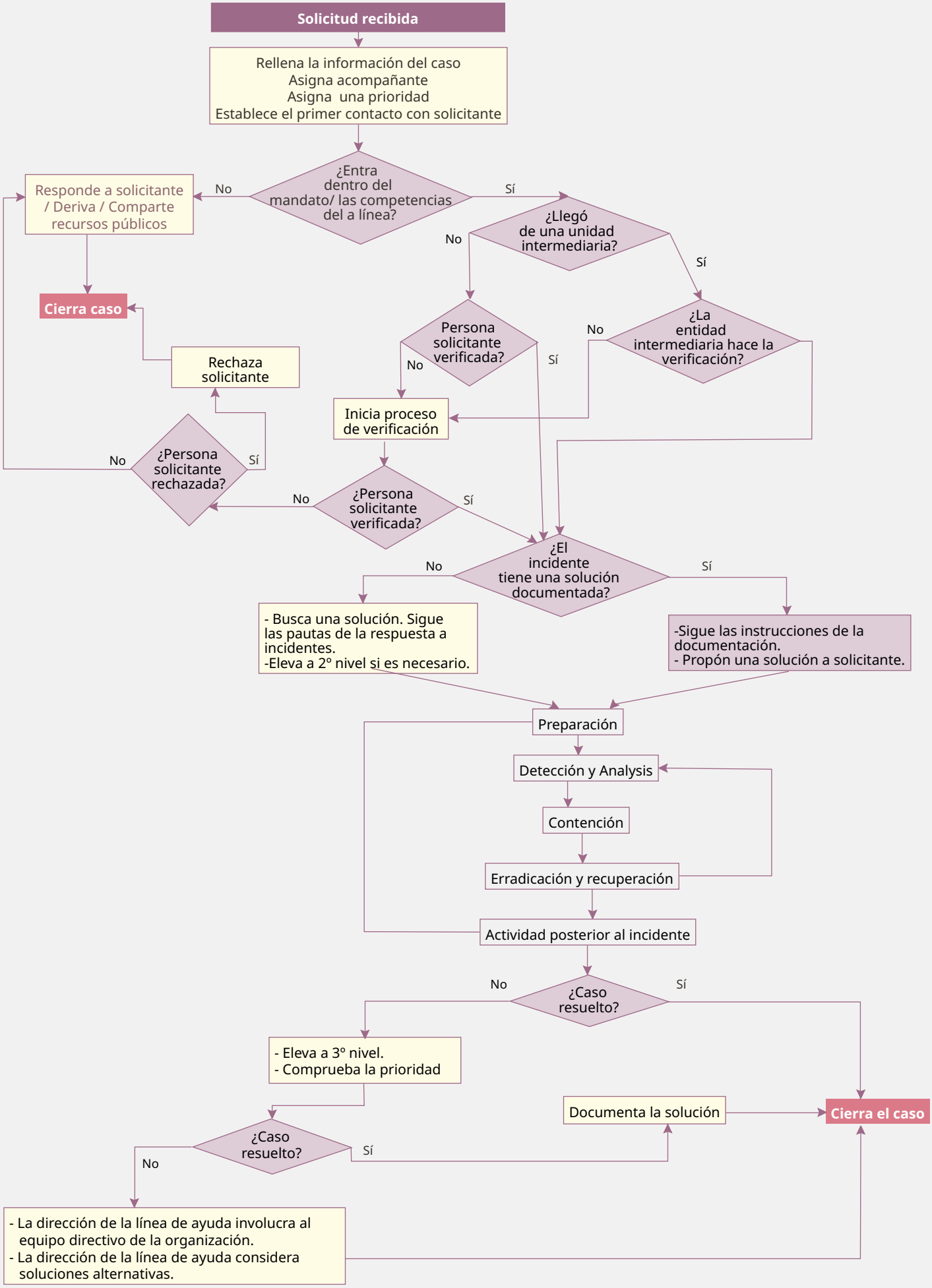
Fase 2: Detección y análisis.

Fase 3: Contención, erradicación y recuperación.

Fase 4: Actividad posterior al incidente.

El proceso de gestión de incidentes no debe limitarse a la fase de contención, erradicación y recuperación: es necesario dar otros pasos, por ejemplo, en la fase de preparación y en la actividad posterior al incidente. Este proceso debe documentarse y organizarse de modo que las personas encargadas de la gestión de incidentes tengan siempre presente cada paso en cada fase del proceso y sean capaces de reducir las posibilidades de que se repita el mismo incidente.Abajo puedes ver un diagrama de flujo que describe el flujo de trabajo de la Línea de Ayuda de Seguridad Digital de Access Now:

Flujo de trabajo de la Línea de Ayuda de Seguridad Digital de Access Now



El proceso de gestión de incidentes también debe adaptarse a las necesidades y al modelo de amenazas del público de una línea de ayuda. Por ejemplo, una LASDSC deberá tener en cuenta que los ataques dirigidos a la sociedad civil suelen ser sofisticados y estar dirigidos a personas que no están preparadas para ellos. Por eso, es importante dedicar tiempo a las fases de preparación y actividad posterior al incidente, para ir más allá de la simple recuperación y convertir un incidente en una oportunidad para prevenir ataques similares en el futuro.

Para saber más

Un ejemplo de un plan de respuesta a incidentes NIST (2012). Computer Security Incident Handling Guide. Disponible en **https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf**. Véase páginas 21-44 para más información sobre el proceso de gestión de incidentes.

Kral, P. (2021). *Incident Handler's Handbook*. SANS Institute. **https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901**.

3.1 Preparación

El proceso de gestión de incidentes comienza cuando se recibe una solicitud: lo primero que hace la persona que está gestionando es anotar la información básica del caso, asignándole una prioridad y una persona que lo acompaña y acusando recibo de la solicitud a la persona solicitante. A continuación, se realiza la verificación obligatoria, para asegurarnos de que tanto la persona solicitante está en la lista de beneficiarias de la LASDSC, como que el servicio solicitado puede ser prestado.

Si la solicitud no entra dentro de las competencias de la LASDSC, se cierra el caso, posiblemente enviando a la solicitante una lista de recursos alternativos disponibles. Si, por el contrario, la solicitud sí entra dentro de las competencias de la LASDSC, se recomienda que el segundo paso preliminar sea la verificación de la beneficiaria. Cada LASDSC debe tener una política de verificación y aplicarla en este paso, para asegurarse de que cada beneficiaria es quien dice ser antes de tramitar su solicitud.

Una vez comprobadas las competencias y realizada la verificación, se inicia el proceso de gestión de incidentes, que también debe prepararse. La fase de preparación implica igualmente la creación de una documentación adecuada que facilite una respuesta rápida a una serie de incidentes identificados, así como la formación del personal para que siga estas instrucciones (véase el apartado 3.5 Documentación de los procedimientos).

La fase de preparación también incluye campañas de divulgación y formación para las beneficiarias que quieran mejorar su seguridad o la de su organización. Durante esta fase, una línea de atención también puede hacer un trabajo de tejer redes y establecer relaciones con proveedores de servicios o asociarse con otras líneas de ayuda y defensoras para refor-

Hemos atendido un mayor nivel de amenazas con un nivel de seguridad y autoridad bajo: nuestras líneas de atención no tienen autoridad sobre las beneficiarias. Podemos recomendar cosas, aconsejarles que hagan otras, pero son ellas quienes deciden si las hacen o no. La mayoría de las veces se trabaja a distancia y es realmente difícil llevar a cabo exactamente lo que nos gustaría hacer, como otros CERT de otros sectores, así que también tenemos que adaptarnos a ello.

Hassen Selmi, Incident Response Lead, Access Now Digital Security Helpline (Entrevista, Noviembre 2021).

zar su capacidad de derivar casos para los que puedan necesitar colaborar con otras entidades.

El trabajo que se invierta en la fase de preparación determinará la rapidez, eficacia y calidad de la respuesta de una LASDSC.

3.2 Detección y análisis

Lo ideal es que el proceso de respuesta a incidentes comience en la etapa de preparación. Sin embargo, siendo realistas, a menudo comienza en la segunda etapa del proceso de gestión de incidentes, cuando se recibe una solicitud de apoyo.

El primer paso de esta etapa es la detección, cuyo objetivo es asegurarse de que lo que la beneficiaria está observando es un verdadero incidente de seguridad digital, es decir, que el comportamiento que ha observado es anormal.

La persona que gestiona el incidente debe pedir a la solicitante toda la información disponible: archivos de registro del sistema y de la red, capturas de pantalla, mensajes de error, informes de antivirus, correos electrónicos sospechosos, síntomas percibidos de cambios en el comportamiento normal y otras evidencias que puedan indicar que un caso es un incidente de seguridad. Las gestoras de incidentes deben estar abiertas a cualquier posibilidad y no dejar pasar por alto ningún incidente de seguridad digital.

Es muy importante que todo el personal de la LASDSC esté familiarizado con el flujo de trabajo, que todo el equipo participe en las distintas tareas y sepa qué hacer cuando se produce un incidente: cómo se maneja y qué hacer en cada fase. Esto debe redactarse, no puede ser una rutina que se dé sin más, porque si no, puede conducir a errores. Este flujo de trabajo no solo lo utilizamos en nuestra línea, sino también otros CERT y está consensuado; además, está estructurado de forma que tiene en cuenta no solo el tipo de beneficiarias a los que ayudamos, sino también nuestras capacidades. Así pues, ayuda a las gestoras de incidentes a saber cómo actuar (desde la detección hasta la recuperación) pero también a prepararse para ello.

Si observamos el diagrama del flujo de trabajo, parece que comienza cuando se inicia el incidente, pero en realidad y en la práctica, la fase de preparación debe desarrollarse de forma continua antes de que se produzca cualquier incidente: es una fase proactiva.

Hassen Selmi, Incident Response Lead, Access Now Digital Security Helpline (Entrevista, Noviembre 2021).

Si la persona que solicita el apoyo padece un trastorno emocional, la recopilación de la información necesaria para determinar de qué tipo de incidente se trata puede resultar revictimizante. En estos casos, se pueden recoger todos los datos con la ayuda de una persona designada por ella.

El siguiente paso en esta etapa es analizar el incidente para comprender mejor qué ocurre y cuáles son las causas. Cuantas más evidencias haya, mejor será la interpretación que pueda hacer la persona que se ocupe de gestionar el incidente.

Distintas evidencias pueden constituir un síntoma del mismo incidente concreto o de otros diferentes. Establecer correlaciones entre las evidencias de forma equivocada puede llevar a una interpretación errónea de los hechos. Una forma útil de evitarlo es llevar a cabo el análisis de forma colectiva en reuniones periódicas de discusión de incidentes.

Una herramienta para empezar a analizar algunas de las cuestiones de seguridad digital más comunes que afectan a la sociedad civil es el **Kit de Primeros Auxilios Digitales** (**https://digitalfirstaid.org**) un recurso gratuito para ayudar a las encargadas de la respuesta rápida a solucionar las emergencias digitales más frecuentes.

Al igual que en la etapa anterior, las personas que gestionan los incidentes deben acordarse de registrar toda la información relevante y documentar todos los pasos realizados.

3.3 Contención, erradicación y recuperación

Una vez confirmado que la beneficiaria está ante un incidente de seguridad digital, la persona encargada de gestionarlo pasará a la fase de contención, erradicación y recuperación. El primer paso es la contención: una intervención para contener el daño y asegurar que el ente atacante ya no pueda acceder a los activos digitales de la beneficiaria. La gestora de incidentes debe proporcionar rápidamente las instrucciones de contención para limitar los daños.

Por supuesto, el procedimiento adecuado para la contención depende del tipo de activo atacado. Para más información sobre los distintos procedimientos, dos buenos recursos de libre acceso son **Access Now Helpline's Community Documentation** (**https://communitydocs.accessnow.org**) y **FemBloc** (**https://docs.fembloc.cat/**).

La erradicación consiste en eliminar todo lo que el ente atacante pueda haber añadido. Esto no siempre es fácil porque los agentes maliciosos suelen ser muy creativos a la hora de idear nuevas formas de atacar.

Posteriormente, la etapa de recuperación tiene como objetivo restaurar los sistemas afectados y tomar las medidas necesarias para evitar nuevos incidentes. La supervisión, por tanto, es fundamental para detectar otros métodos que pueda utilizar un ente atacante y cualquier otra exfiltración de datos. Debido a que las líneas de ayuda de la sociedad civil a menudo no pueden supervisar directamente los activos de las personas beneficiarias, se puede sustituir este paso formando a las beneficiarias para que lo puedan hacer ellas mismas.

A veces, quien acompaña un caso carece de tiempo o capacidad para poder cerrarlo. En estos casos, se puede requerir la participación de otras personas del equipo para externalizar la gestión del caso o parte de ella, en especial el análisis. Esta es una de las situaciones en las que la creación de redes y la colaboración entre las LASDSC puede ser especialmente útil (ver Capítulo 4 para mas detalles).

Los últimos pasos también forman parte del proceso. Si a las personas que gestionan los casos se les ocurre una nueva solución o se dan cuenta que las instrucciones que aparecen en la documentación no son tan eficaces como quisieran para gestionar ese incidente, se les pide que propongan soluciones a partir de lo que han observado. A veces también se puede sugerir antes del propio proceso, cuando te das cuenta de que un procedimiento no va a funcionar realmente y que es preciso mejorarlo.

Hassen Selmi, Access Now Digital Security Helpline (Entrevista, Noviembre 2021).

3.4 Actividad posterior al incidente

La última etapa del proceso de gestión de incidentes tiene como objetivo recopilar lo que la persona que ha gestionado el incidente ha observado mientras trabajaba en el caso. Aunque es posible que se hayan detectado oportunidades para mitigar incidentes de seguridad digital habituales y se hayan transmitido a la beneficiaria, también es posible que hayan surgido nuevas formas de abordar un problema, que deben documentarse.

Estas lecciones aprendidas mejorarán la documentación de la línea de atención gracias a un planteamiento más creativo y preciso de la gestión de incidentes. Se recomienda no retrasar el proceso de documentación una vez cerrado el caso, pues los pequeños detalles tienden a olvidarse. A veces, un incidente puede estar conectado con una serie de ataques de los que hay que advertir a otros grupos: por ello, en esta fase, es importante la divulgación y la creación de redes para difundir las alertas públicas y avisar de este tipo de incidentes a otros objetivos potenciales.

3.5 Documentación de los procedimientos

El término "documentación" es bastante amplio. Puede referirse a distintas cosas y, si no se define claramente, puede dar pie a la confusión. En la respuesta a incidentes, hay dos tipos distintos de documentación, ambas igual de importantes: la documentación de casos y la de procedimientos.

La documentación de los casos suele realizarse a través de un gestor de tickets (véase la sección 2.5 Infraestructura y herramientas en el Capítulo 2) u otras plataformas seguras. Consiste en anotar todas las comunicaciones con la beneficiaria, así como la solución técnica que se adoptó para resolver el caso, las evidencias o pruebas que se recogieron, los motivos por los que se plantearon esas soluciones y los recursos que se consultaron. Esto permite rastrear cómo se ha resuelto un caso y, si se descubre una nueva solución, tiene lugar el segundo tipo de documentación.

El segundo tipo de documentación, que se desarrolla durante la fase de preparación del proceso de gestión de incidentes y se revisa durante todo el ciclo, es la documentación de procedimientos. Se trata de la documentación técnica que contiene las estrategias para atender los incidentes que sufre nuestro público.

En el trabajo de una LASDSC, la documentación de los procedimientos es fundamental para asegurarse de que los incidentes se gestionan correctamente y se garantice la calidad. Gracias a ella, el equipo puede contar con una base de conocimientos actualizada permanentemente que servirá para agilizar su respuesta. Por lo tanto, la información de la que disponen las gestoras de incidentes debe ser precisa, estar actualizada y ser de fácil acceso.

Este capítulo se centrará en los distintos aspectos a tener en cuenta a la hora de crear la documentación de los procedimientos de gestión de incidentes: los principios rectores, la planificación, las plataformas y los formatos, las estrategias de colaboración y las guías de estilo.

En la fase de preparación del proceso de gestión de incidentes procuramos tener un conjunto de documentos o guías que nos permitan responder a una serie de incidentes que tenemos identificados, que entendemos o que han ocurrido en nuestra línea de ayuda o en otras organizaciones o CERT. Por eso, intentamos tenerlos siempre a mano, formamos al personal para que los siga y cuando se produce un incidente que cumple los criterios recogidos en estos, los consultamos. Si existe documentación para un determinado tipo de incidente, la persona que está gestionando el caso debe seguirla.

Hassen Selmi, Access Now Digital Security Helpline (Entrevista, noviembre de 2021).

Principios básicos de la documentación técnica

La creación y el mantenimiento de una base de conocimientos técnicos de la LASDSC es una labor de colaboración continua tanto en los CERT y las líneas de ayuda específicas como entre la comunidad de organizaciones de seguridad digital para la sociedad civil. Esta labor colaborativa ha llevado a la adopción de algunas de las mejores prácticas establecidas en la industria tecnológica.

Tanto si se trata de una guía para usuarias finales de una aplicación telefónica, como de una entrada para la base de conocimientos incluida en el gestor de tickets de una línea de ayuda de seguridad digital, cualquier tipo de documentación técnica debe ser:

- **Participativa**: debe incluir a todas las personas que la van a utilizar, por lo que tiene que ofrecer formas sencillas de contribuir y registrar todos los cambios.
- **Actualizada**: una documentación incorrecta puede inducir a más errores que la falta de documentación.

- **Única**: debe guardarse en un único lugar para evitar incoherencias entre versiones.
- **Localizable**: debe ser posible encontrar la documentación cuando se necesite.
- **Comprensible para las usuarias finales**: debe evitarse la jerga técnica.
- **Protegida de intentos no autorizados de modificar su contenido.**
- **Fácil de reproducir para otros proyectos**.
- **Fácil de utilizar en diferentes formatos**: sitios web, aplicaciones para móviles o archivos PDF, entre otros.

Planifica la creación de nueva documentación

Una LASDSC puede documentar soluciones técnicas tanto para las personas que se encargan de gestionar los incidentes como para las beneficiarias, pero a veces también puede ser necesario escribir para colaborar con socias, realizar campañas de incidencia, comunicarse con los medios, etc. Especialmente en el caso de que una documentación se dirija a usuarias sin formación técnica, siempre conviene preguntarse si la solución específica que se quiere documentar no ha sido ya presentada por otros sitios web de seguridad digital de confianza. Si es así, en lugar de escribir desde cero, se puede, por ejemplo, enlazar un buen recurso a tu base de conocimientos.

Antes de empezar a escribir, una buena práctica es analizar la documentación existente, tanto para asegurarse de no duplicar esfuerzos como para tener una idea clara de las soluciones técnicas necesarias para resolver un incidente concreto.

Cuando tengas una idea clara de lo que quieres escribir, intenta elaborar la nueva documentación de forma que pueda utilizarse en otros casos y no sea específica de un caso que acabas de atender. Para ello, puedes responder a las siguientes preguntas:

¿A quién está dirigido?

¿Vas a enviar esta documentación a cada una de las beneficiarias por correo electrónico o vas a publicar un aviso en tu sitio web para que todo el mundo pueda leerlo? También puede estar dirigido a gestoras de incidentes que trabajan en otras organizaciones, a alguien que esté llevando a cabo una campaña de incidencia política o incluso puede ser para una ponencia en una conferencia especializada.

¿Qué se quiere lograr?

¿Quieres que las gestoras de incidencias dispongan de soluciones técnicas rápidas para los casos que tratan? ¿O estás redactando una plantilla para los mensajes que envías de forma habitual a tus beneficiarias? ¿Estás preparando un aviso de seguridad para advertir a todas las beneficiarias sobre un nuevo tipo de ataque digital? ¿O quieres preparar un informe público que pueda enviarse a los medios de comunicación?

¿Qué tipo de contenido responde mejor a las necesidades de tu público?

Ten en cuenta el contexto de tu público. ¿Son profesionales de la informática o usuarias sin formación técnica? ¿Necesitan información técnica precisa o unas instrucciones sencillas paso a paso con capturas de pantalla? ¿Necesitas añadir imágenes a tu guía o sería mejor crear un vídeo o una infografía?

¿Cómo encontrará tu público el contenido?

¿Incluirás este contenido en tu gestor de tickets? ¿Se publicará en tu sitio web? ¿Estás creando un manual que se convertirá en un PDF imprimible o en una aplicación para dispositivos móviles? ¿El contenido estará disponible tanto en línea como fuera de línea?

¿Se traducirá o adaptará el contenido?

En función del público al que vaya dirigido, puede que quieras traducir el contenido a los idiomas y referencias culturales más utilizados por las personas a las que quieres llegar.

Estas preguntas te ayudarán a definir el contenido, el estilo y el formato de tu documentación. Por ejemplo:

- Si tienes que alertar a tu público sobre una nueva amenaza, escribe rápidamente y pule el mensaje más tarde.
- Si el presupuesto y los plazos son ajustados, se puede optar por compartir un texto sencillo con las personas implicadas lo antes posible y pensar en un formato más bonito cuando se disponga de recursos.
- Si el público es numeroso y el tema es complejo, quizá sea útil hacer un vídeo corto con subtítulos.
- Si estás escribiendo instrucciones técnicas para gestoras de incidentes, debes incluir detalles técnicos y publicar la documentación en la misma plataforma en la que las gestoras de incidentes documentan los casos para que esté disponible (por ejemplo, un gestor de tickets).
- Si estás escribiendo documentación que puede ser utilizada por otras organizaciones de la sociedad civil, utiliza un lenguaje sencillo, fácil de traducir y publícala con una licencia y en un formato que permitan la reutilización.

Plataformas y formatos para la documentación técnica

La herramienta que más utiliza tanto la industria informática como el movimiento que ofrece protección digital a la sociedad civil para elaborar documentación bajo los principios orientativos mencionados, es git, una tecnología para el control de versiones. En la mayoría de los casos, se utiliza con **Markdown** (**https://daringfireball.net/projects/markdown/**), un lenguaje de marcado sencillo y un generador de sitios estáticos para cargar el contenido en un sitio web con capacidad de búsqueda y fácil de usar.

Git para control de versiones

Git es el *software* de control de versiones más utilizado para escribir documentación técnica de forma colaborativa. Su principal característica es que permite hacer un seguimiento de los cambios realizados en cada uno de los archivos de una carpeta, por lo que existe un registro de cada una de las ediciones. También permite revertir los cambios a una versión específica, si es necesario.

Git facilita la colaboración porque permite fusionar los cambios realizados por varias personas en una sola fuente. Otra característica útil de este *software* es la posibilidad de proteger la identidad de quienes colaboran gracias a la opción de crear repositorios privados a los que solo puede acceder un grupo seleccionado de personas usuarias. Además, permite informar sobre las incidencias, gestionar las personas que colaboran, asignar diferentes roles, documentar el proceso, acceder a las estadísticas, etc.

La documentación gestionada en repositorios git suele estar alojada en plataformas de terceros como **Github**, **Gitlab** o **0xacab**, o en instancias autogestionadas de Gitlab. Algunos ejemplos de documentación desarrollada de forma colaborativa por la sociedad civil utilizando git son:

- Documentación para la comunidad de la línea de ayuda en seguridad digital de Access Now (**https://communitydocs.accessnow.org/**), que se encuentra en este repositorio de Gitlab.com (**https://gitlab.com/AccessNowHelpline/community-documentation**).
- Digital First Aid Kit (**https://digitalfirstaid.org**), que se encuentra en este repositorio de Gitlab.com (**https://gitlab.com/rarenet/dfak**).

- Documentación técnica de la la línea de atención feminista Fembloc (**https://docs.fembloc.cat/**), disponible en este repositorio de Gitlab (**https://gitlab.com/FemBloc-HL/shared-documentation).**

Hay muchos recursos en línea para aprender a usar git. Busca hasta encontrar el que mejor se adapte a tus necesidades de aprendizaje. La guía **git - the simple guide** puede ser un buen punto de partida. Aunque git no es complejo para una persona que colabora de forma habitual, se requiere cierta experiencia para familiarizarse con su lógica y sus comandos.

Markdown para escribir

En todos los ejemplos anteriores, los documentos están escritos en **Markdown**, un lenguaje de marcado ligero creado por Aaron Swartz y John Gruber en 2004 para permitir que la gente "escriba utilizando un formato de texto plano fácil de leer y de escribir, con la opción de convertirlo a un XHTML (o HTML) estructuralmente válido" **(Daring Fireball, 2004)**

Los documentos de Markdown pueden convertirse a muchos formatos diferentes, lo que permite crear sitios web, aplicaciones para móviles, libros electrónicos y PDF a partir de la misma fuente.

Es importante recordar que, aunque la mayoría de los proyectos impulsados por organizaciones de la sociedad civil utilizan Markdown, para la documentación técnica se emplean otros lenguajes de marcado, en especial **AsciiDoc** y **reStructuredText** (**reST - https://www.sphinx-doc.org/en/master/usage/restructuredtext/**).

Si es la primera vez que utilizas Markdown, puedes tener a mano la guía de sintaxis como referencia:

- Sintaxis básica de Markdown (**https://tutorialmarkdown.com/sintaxis**).
- Hoja de trucos de Markdown (**https://www.markdownguide.org/cheat-sheet**).
- Guía Markdown (**https://www.markdownguide.org/basic-syntax**).
- Sintaxis básica de escritura y formato Markdown en Github (**https://docs.github.com/es/get-started/writing-on-github/getting-started-with-writing-and-formatting-on-github/basic-writing-and-formatting-syntax**).

Generadores de sitios estáticos para publicar sitios web

Para convertir Markdown en sitios web con capacidad de búsqueda, se suelen utilizar generadores de sitios estáticos como **Jekyll** (**https://jekyllrb.com/**), **Gatsby** (**https://www.gatsbyjs.com/**) o **Metalsmith** (**https://www.metalsmith.io/**).

Los generadores de sitios estáticos (SSG, por sus siglas en inglés) son una alternativa a los sistemas de gestión de contenidos como WordPress o Drupal, donde el contenido se gestiona y almacena en una base de datos en el servidor web. Es decir, en lugar de obtener el contenido de una base de datos cada vez que hay una solicitud de contenido web, los SSG generan todo el sitio web después de cada actualización y crean un árbol de archivos HTML listo para ser visitado.

Una gran ventaja de esta infraestructura basada en git es que es relativamente sencilla de mantener. Los sitios estáticos son resistentes al troleo y a los frecuentes ataques que se dan en plataformas como los wikis (sobre todo si permiten la edición por parte de cualquier persona usuaria) u otras aplicaciones web o sitios dinámicos que requieren mucho trabajo para mantener la seguridad y asegurarse de que el contenido no se edita de forma maliciosa o por error.

Documentación colaborativa

La utilización de una infraestructura de documentación en git facilita que cualquier otra línea de ayuda o persona que tenga acceso a ese repositorio git pueda utilizar la misma base de conocimientos para crear su propio sitio web, aplicación móvil, libro electrónico, etc., y también para recibir y enviar actualizaciones a la misma.

Esto es posible gracias a la propia arquitectura de los *hubs* de alojamiento en git, como Gitlab o Github, que permite **hacer una copia de un proyecto** y enviarle solicitudes de fusión (o *merge requests*) después de que se haya modificado en la copia o *fork*. Ante la escasez de recursos disponibles en el ámbito de la sociedad civil para crear documentación técnica que se actualice constantemente, colaborar en recursos de documentación técnica compartidos se ha convertido en una práctica habitual. Para ello, hay que evitar los formatos que no son fáciles de descargar y duplicar y que no están sujetos al control de versiones, como los wikis, los sitios web, los documentos alojados en Google Drive o los PDF, y utilizar licencias de contenido que permitan la colaboración y la creación de obras derivadas.

El sistema de colaboración también permite evitar la duplicación de esfuerzos, ya que los recursos existentes pueden reutilizarse en lugar de tener que empezar a escribir desde cero más de una vez.

Guías de estilo

La documentación de los procedimientos técnicos de las LASDSC debe redactarse en un lenguaje fácil de leer e inclusivo, teniendo en cuenta que quienes gestionan los incidentes en general no hablan inglés como lengua materna y que ninguna persona es experta en todo, especialmente en el ámbito de la sociedad civil.

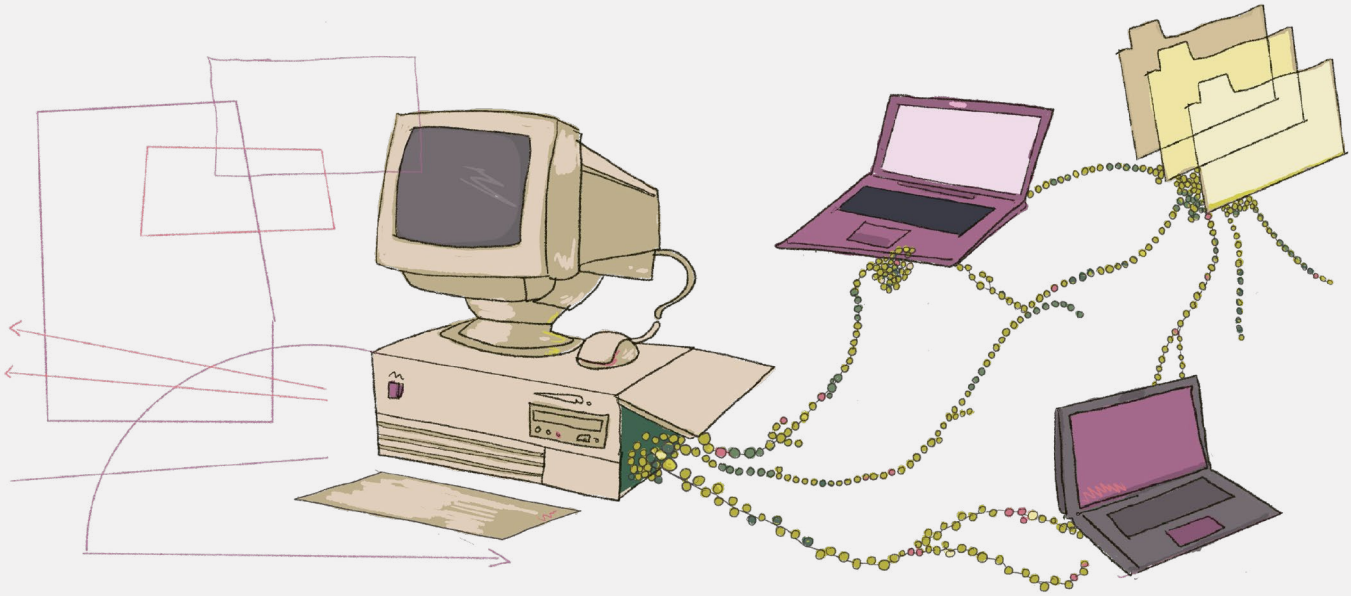
Antes de comenzar a desarrollar de cero, colaborar o mantener documentación técnica, se recomienda seguir algunas normas básicas que facilitan la lectura y comprensión del texto:

- Usar frases cortas que suenen naturales y sean sencillas.
- Optar, en la medida de lo posible, por palabras comunes: no utilizar jerga o acrónimos, a menos que sea realmente necesario (y en ese caso, es necesario explicarlos, al menos, una vez).
- Incluir a todos los géneros utilizando palabras y pronombres de género neutro.
- Utilizar voz activa (sujeto + verbo + objeto) siempre que sea posible.
- Las listas son un buen recurso para visualizar la información de forma rápida.
- Enlazar recursos externos útiles en caso de que la persona beneficiaria necesite profundizar sus conocimientos sobre un tema.

Existen muchos recursos sobre cómo redactar una buena documentación técnica. Aquí mencionamos tan solo unos pocos:

- Una lista de recursos de escritura técnica - Google (**https://developers-google-com.translate.goog/tech-writing/resources?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=wapp**).
- Redacción de documentos técnicos - Guía paso a paso (**https://www.socialmediapymes.com/redaccion-de-documentos-tecnicos/**).
- Guía para una comunicación no sexista e inclusiva - Fundación Adsis (**https://www.fundacionadsis.org/sites/default/files/guia_comunicacion_nosexista_inclusiva.pdf**).

4



Más allá de tu equipo: trabajo en red y control de calidad

Los ataques digitales no cesan de evolucionar, ampliando su radio de acción y agravando su impacto, al igual que los contextos políticos en los que se mueven las personas que defienden los derechos humanos y activistas. Estar al día de los cambios, comprenderlos y elaborar estrategias de respuesta puede requerir mucho tiempo y recursos.

Crear y mantener una comunidad de práctica es fundamental para una línea de atención, ya que facilita la colaboración. Además, agiliza los mecanismos de derivación, fomenta el conocimiento de las realidades de todas las regiones, el intercambio de recursos, el aprendizaje de nuevos enfoques y la realización de investigaciones y estudios colaborativos. Cada línea de atención o CERT puede especializarse en un tipo de ataque o público concreto de modo que el resto de la comunidad pueda beneficiarse de esos conocimientos.

También es importante actualizarse constantemente, comprobar que los procedimientos que siguen quienes gestionan las incidencias son los adecuados y recibir observaciones y *feedback* de forma continua de organizaciones y personas aliadas y de las beneficiarias para mejorar el flujo de trabajo de la línea de atención.

Este capítulo se centra en las derivaciones (una estrategia de colaboración común entre las líneas de atención y los CERT que permite mejorar la capacidad de respuesta) y en el control de calidad (con recomendaciones sobre diferentes enfoques y mecanismos para supervisar, mantener y mejorar la calidad de los servicios prestados).

4.1 Crea y cuida tu red de socias

Para tener más opciones de derivación, es importante construir una red de confianza que dé visibilidad al propio trabajo y que aprenda más sobre el trabajo de sus pares. Esto se puede conseguir, por ejemplo, participando en eventos locales o internacionales. Pueden presentar su trabajo en charlas relámpago, *tech demos*, laboratorios comunitarios, talleres, etc. Consulten el listado de conferencias en el capítulo 2 (sección de Formación y desarrollo profesional) para decidir a cuáles pueden asistir.

Formar parte de listas de correo como la lista de correo encriptada de **CiviCERT** es una gran ventaja, por ejemplo, a la hora de hacer derivaciones. Esta comunidad que vela por la seguridad digital de la sociedad civil suele intercambiar conocimientos sobre derivaciones y experiencia en respuestas rápidas. Más información sobre cómo unirse a la red en su **sitio web** (**https://www.civicert.org/apply-to-be-a-member/**).

No hace falta recordar que formar parte de una red o comunidad es un compromiso proactivo. Las comunidades necesitan que se las cuide y cultive. Es decir, requieren el mantenimiento de su infraestructura y documentación, la facilitación de encuentros, recursos, divulgación, intercambio y, sobre todo, tiempo. Es importante tenerlo en cuenta a la hora de planificar las horas y actividades del equipo.

La detección de necesidades en las peticiones de apoyo que recibíamos nos llevó a crear puentes con plataformas en línea para tratar de frenar la violencia. Nos dirigimos directamente a ellas y nos abrieron sus puertas, en parte porque había información que les interesaba o porque querían conectar con organizaciones que pudieran mediar. Tuvimos que ser estratégicas y limitar la información que compartíamos porque la utilizaban en su beneficio. Si lo que nos ofrecían no servía para mejorar las condiciones de atención a las mujeres, no nos interesaba. Aunque sean grandes empresas, esperamos reciprocidad en las colaboraciones.

Luchadoras (Haché, 2021).

4.2 Derivaciones

A veces, una LASDSC recibe una solicitud que no puede atender, ya sea porque no se ajusta a su ámbito de actuación o porque requiere una serie de conocimientos de los que carece. La LASDSC puede derivar el caso a otra entidad que pueda proporcionar el apoyo necesario en tales situaciones.

Tras verificar la identidad de la persona solicitante y en función de su solicitud, existen cuatro tipos de contactos a los **que derivar**:

- **Otra ONG o entidad sin fines de lucro** - Puede ser una derivación a una organización sin fines de lucro de confianza, conocida o con la que se haya trabajado en el pasado.
- **Empresas privadas** - También se puede derivar a una empresa privada con una política de privacidad y modelo de negocio éticos, una empresa de confianza o familiarizada con los desafíos de las organizaciones sin fines de lucro y que utilice tecnologías de código abierto, transparentes y auditables.
- **Entidades gubernamentales** - Es posible que tengan que redirigir el caso a instituciones gubernamentales como un CERT nacional.
- **Especialistas independientes** - También se puede derivar a una beneficiaria a una persona de la comunidad de especialistas en seguridad digital que esté familiarizada con las necesidades específicas de las personas que defienden los derechos humanos.

A continuación, se ofrece una lista de posibles apoyos dentro de la comunidad de seguridad digital o cercanos a la misma, una vez identificada la necesidad de la persona solicitante. Verificar a la persona solicitante es una buena práctica cuando se deriva al sitio web de una organización afín, pero no es obligatorio en este caso.

Equipos CERT (instituciones gubernamentales)

* Equipos FIRST (**https://www.first.org/members/teams/**).

Prevención de ataques DDoS

* Deflect (**https://deflect.ca/**).
* CloudFlare Galileo (**https://www.cloudflare.com/galileo/**).
* Google Project Shield (**https://projectshield.withgoogle.com/landing?hl=es**).

Dominios y alojamiento

* Consejos sobre alojamiento en Documentación para la comunidad de la línea de ayuda de Access Now. (**https://accessnowhelpline.gitlab.io/community-documentation/88-Advice_Hosting.html**).

Apoyo en caso de emergencia

* Kit de Primeros Auxilios Digitales, un mecanismo de entrada para llegar a integrantes de la comunidad CiviCERT (**https://digitalfirstaid.org/es/support/**).
* Committee to Protect Journalists, para periodistas (**https://cpj.org/emergency-response/how-to-get-help/**).

Financiación y licencias gratuitas

* DDP Incident Emergency Fund (**https://www.digitaldefenders.org/funding/incident-emergency-fund/**).
* OTF Funds (**https://www.opentech.fund/funds/**).
* TechSoup (**https://www.techsoup.org/**)
* Google Nonprofits (**https://www.google.com/nonprofits/**).

Documentación sobre violaciones de derechos humanos

* Huridocs (**https://huridocs.org/**).
* Witness (**https://www.witness.org/**).

Apoyo jurídico

* Media Defence (**https://www.mediadefence.org/**).

Seguridad física y reubicación

* Protect Defenders (**https://protectdefenders.eu/protecting-defenders/**).
* Umbrella (app para móviles - **https://secfirst.org/umbrella/**).

Evaluaciones de vulnerabilidad y pruebas de penetración

* Red Lab de OTF (**https://www.opentech.fund/labs/red-team-lab/**).

Formación

* Recursos de formación y referencias en Documentación para la comunidad de Access Now (**https://accessnowhelpline.gitlab.io/community-documentation/301-Training_Resources.html**).

Proceso de derivaciones

Verificación

La verificación de la persona solicitante y de su organización es obligatoria cuando se deriva directamente a otro equipo. Durante este proceso, es preciso asegurarse de que se ha verificado la autenticidad de la solicitud y el trabajo de la persona beneficiaria. La verificación de una organización o persona es una oportunidad para ampliar la red de confianza de su línea y de la comunidad.

Triaje

Antes de derivar a la organización o persona adecuada, es importante evaluar las necesidades de la persona solicitante. Lo primero que hay que hacer es analizar la amenaza y el incidente que está sufriendo. Se puede utilizar **un enfoque de modelo de amenazas o de evaluación de riesgos** (**https://accessnowhelpline.gitlab.io/**

community-documentation/200-Lightweight_Security_Assessment.html) como punto de partida. Este triaje inicial ayudará a determinar a quién derivar a la persona beneficiaria.

Identificación de la derivación apropiada

Los criterios para elegir una derivación se deben basar en:

- Las necesidades de la persona que lo solicita.
- El idioma de la persona beneficiaria.
- El contexto geopolítico.
- Los conocimientos técnicos necesarios.
- El coste de la derivación.

Consentimiento para la derivación

Se recomienda informar a la persona beneficiaria desde el principio sobre la intención de derivarla a otra persona/entidad. Para cumplir con el acuerdo de confidencialidad entre la LASDSC y la persona solicitante, es preciso pedirle formalmente su aprobación para compartir información con otras personas (sobre la evaluación de vulnerabilidad, identidad y datos de contacto de la beneficiaria, etc.).

Comunicar a la persona solicitante las razones principales por las que se inclinan por una entidad concreta, su experiencia, así como las razones principales por las que no pueden satisfacer su solicitud, puede ayudarla a tomar una decisión. También es fundamental indicar si la entidad a la que se deriva el caso tiene capacidad para prestar servicios gratuitos.

Consentimiento de la tercera parte a la que se deriva el caso

Una vez identificada la entidad/persona adecuada para la derivación y tras el visto bueno de la persona solicitante, podrán compartir los detalles sobre:

- La evaluación de las necesidades de la solicitante.
- El modelo de amenaza de la solicitante.

El objetivo es asegurarse de que la tercera parte a la que se remite a la persona solicitante tiene suficiente información para asumir la gestión de la solicitud. Si no puede ofrecer un servicio gratuito, habrá que definir los siguientes detalles:

- Qué servicio se ofrecerá.
- El coste del servicio.

Para que la derivación funcione, habrá que aclarar estos aspectos de antemano para que las expectativas de la persona beneficiaria y de la tercera parte coincidan.

Establecer el contacto

A la hora de poner en contacto a la persona solicitante y a la entidad/persona a la que se deriva, intenta identificar un canal de comunicación seguro con el que ambas estén familiarizadas. Si utilizan PGP, valoren la posibilidad de que compartan sus claves PGP cuando se presenten.

Seguimiento

Transcurrido un tiempo (en función de la carga de trabajo, pueden ser un par de semanas o unos meses) es una buena práctica comprobar tanto con la persona bene-

ficiaria como con la tercera parte, que el caso se ha resuelto y que sus necesidades se han satisfecho.

Derivar un caso abierto

Puede ocurrir que hayan empezado a ayudar a una persona en situación de riesgo pero que, por diversas razones, ya no le puedan seguir prestando asistencia.

En estas situaciones, lo mejor es derivarla a una persona/entidad de confianza. El proceso de derivación seguirá los pasos que se indican en esta sección, pero debe incluir un paso adicional a la hora de entregar el incidente y un esfuerzo adicional de comunicación para gestionar las expectativas.

A la hora de informar a la entidad/persona de confianza la intención de derivarle una solicitud:

- Tengan en cuenta que, en este caso, la gestión de las expectativas es fundamental.
- Es preferible tener preparada una lista de posibles derivaciones para estos casos.
- Aclaren los detalles económicos.

Cuando acuerden con la solicitante la derivación:

- Expliquen por qué es preciso derivarle.
- Den detalles sobre la experiencia de su socia.

Durante el proceso de derivación:

- Entreguen a su socia toda la información que han recopilado y su evaluación técnica.

4.3 Intercambio de información sobre amenazas

Es una buena práctica compartir regularmente con su comunidad información anonimizada sobre los casos que han tratado. Este intercambio facilitará que otras organizaciones comprendan e identifiquen las pautas y tendencias de ataques digitales que también pueden afectar a sus beneficiarias.

En CiviCERT la información sobre el trabajo de cada integrante se comparte semestralmente en torno a las siguientes cuestiones:

Información sobre amenazas

- ¿Qué tipo de casos de respuesta rápida han atendido en el último periodo de tiempo?
- ¿Cuál fue la naturaleza de los ataques?
- ¿Quién era el objetivo?
- ¿Qué tendencias observan en su trabajo?

Inteligencia sobre amenazas

- ¿Qué amenazas y/o tendencias recientes les preocupan más?
- ¿Ha cambiado algo en los ataques que han estado supervisando/atendiendo?
- ¿A qué deberían prestar atención otros equipos de respuesta rápida?

Recuerden que la anonimización de esta información debe hacerse de forma que sea imposible rastrear el caso.

4.4 Control de calidad

Este proceso describe los estándares de calidad recomendados para una línea de atención. También ofrece recomendaciones sobre distintas perspectivas y mecanismos que pueden utilizarse para supervisar, mantener y mejorar la calidad de los servicios prestados.

Estándares de calidad

Para medir y evaluar la calidad de su trabajo es importante definir las expectativas y normas que utilizará la LASDSC. A la hora de evaluar la calidad del servicio deben tener en cuenta las siguientes pautas:

- Es importante crear un espacio donde las personas beneficiarias e intermediarias se sientan acogidas, comprendidas, seguras y protegidas.
- Una línea de atención debe ser clara, fiable y práctica. El servicio de atención debe ser excelente y debe prestarse demostrando comprensión y empatía con las necesidades de las beneficiarias y su situación.
- Las beneficiarias deben ser tratadas con dignidad, respeto y confidencialidad para que se sientan protegidas y seguras de que su problema está siendo atendido.
- Escuchar es lo primero. Sean pacientes y escuchen siempre lo que las beneficiarias tienen que decir antes de sacar conclusiones precipitadas y dar consejos técnicos.
- Utilicen un lenguaje claro, inclusivo y no sexista, ni racista, clasista o colonialista al escribir o hablar.
- Las encargadas de gestionar los incidentes deben adoptar un enfoque basado en estrategias de aprendizaje de personas adultas. Siempre que sea posible, el objetivo de las interacciones debe ser educar y empoderar a las personas beneficiarias mediante el conocimiento y el asesoramiento.
- Las interacciones con las beneficiarias deben ser claras y concisas. Pueden proceder de entornos diversos y tener distintos niveles de conocimientos técnicos.
- Definan cuál será su **Acuerdo de nivel de servicio** (ANS - **https://es.wikipedia.org/wiki/Acuerdo_de_nivel_de_servicio**), que incluye un tiempo máximo de respuesta para las solicitudes entrantes. Por ejemplo: “en días laborables, responder a todas las solicitudes dentro de las dos primeras horas desde que se reciben, durante el horario laboral; en el fin de semana, en un plazo de 24 horas”.
- Mientras el caso esté abierto, respondan con rapidez. Si una beneficiaria no responde, comprueben periódicamente que sus necesidades están cubiertas.
- Se debe utilizar la documentación existente, los procesos de derivación y otros mecanismos para ofrecer soluciones técnicas de calidad, razonables y adecuadas.

Mecanismos de control de calidad

Define roles y responsabilidades

Para poder garantizar la calidad del servicio, hay algunos roles que deben ser definidos por la LASDSC.

Acompañante: La persona que dirige el caso y trabaja para ayudar a la beneficiaria con su solicitud.
Revisora: La persona encargada de revisar la calidad del trabajo. Puede ser la misma persona siempre, o puede rotar entre el equipo, dependiendo del tamaño y la estructura de la LASDSC. En el caso de organizaciones grandes, puede haber más de una persona encargada de la revisión.

Define un período de tiempo

Las revisiones de casos deben realizarse con regularidad para que sean eficaces. Definan la frecuencia con la que se realizarán estas revisiones. La periodicidad puede variar: desde revisiones semanales a mensuales, trimestrales o incluso anuales. La periodicidad dependerá del tamaño de la LASDSC, de su capacidad de personal, del número de solicitudes tramitadas, del tipo de solicitudes, etc.

Revisión de casos individuales

Proceso

La persona encargada de la revisión llevará a cabo una revisión de los casos cerrados por las personas acompañantes durante el periodo de tiempo especificado, de acuerdo con las necesidades de la LASDSC.

La revisión debe ser flexible en cuanto al momento en que se realiza, pero al final de cada periodo todos los casos cerrados deben haber sido revisados.

Para facilitar el trabajo de revisión y lograr revisiones más valiosas y útiles, las personas acompañantes deben documentar cada caso de forma exhaustiva. Valoren la posibilidad de añadir metadatos específicos a la documentación del caso para hacer un seguimiento de los comentarios y las apreciaciones de cada caso. Anoten también cualquier comentario o mejora que pueda producirse en el propio proceso de revisión.

La LASDSC debe tener en cuenta los resultados de las revisiones para mejorar sus políticas, el proceso de gestión de incidentes, los protocolos de atención y las competencias del equipo.

Criterios

La revisión tendrá en cuenta los siguientes aspectos:

Metadatos

- ¿Están completos todos los metadatos del caso?
- ¿Es el contenido de los metadatos detallado y preciso?

Puntualidad

- ¿Se envió la primera respuesta dentro del ANS?
- ¿Se ha realizado un seguimiento regular?
- ¿Recibió la beneficiara las respuestas a tiempo?

Idioma

- ¿Fueron claras las comunicaciones con la beneficiaria?
- ¿La estructura, ortografía y gramática de las comunicaciones es adecuada?
- ¿Se ha utilizado un lenguaje no violento y de género neutro? ¿Se adoptó un enfoque interseccional?

Eficiencia

- ¿Se sometió a la beneficiaria a una evaluación de riesgos antes de recomendar una solución?
- ¿Fue la solución utilizada la más adecuada para el contexto de la beneficiaria?

Documentación

- ¿Se ha documentado correctamente el caso?
- ¿Se registró correctamente la información adicional (capturas de pantalla, análisis, archivos) del caso?

Servicio de atención

- ¿Se ha procurado validar el relato de la beneficiaria?
- ¿Se sintió empoderada la beneficiaria cuando se resolvió el caso?

Recomendaciones técnicas

- ¿Se aplicó la solución tecnológica adecuada en este caso?
- ¿Se comunicó la información técnica de forma que se ajustara a las capacidades y necesidades de la beneficiaria?

Retroalimentación

Una buena forma de prestar regularmente un buen servicio es poner en marcha algún mecanismo para recabar la opinión de la beneficiaria una vez resuelto el caso. Esta retroalimentación puede recogerse de distintas maneras, dependiendo de las necesidades y capacidades de su organización. Algunos ejemplos son:

- Formularios en línea
- Mensajes de seguimiento
- Llamadas de evaluación

Es importante tener en cuenta que la información recopilada durante esta etapa puede ser sensible, por lo que es necesario garantizar que se transfiera y almacene de forma segura.

Proceso de revisión de las evaluaciones

Si se recogen comentarios y opiniones, la persona encargada de la revisión debe estudiarlos y detectar posibles áreas de mejora de los procesos.

A continuación, debe encontrar una forma adecuada de informar a la persona que ha acompañado el caso sobre esta retroalimentación (ya sea positiva o negativa) y valorar si el caso en cuestión necesita más medidas.

Referencias

Access Now Digital Security Helpline (2018). *Documentation for FIRST Site Visit.* Confidencial.

Carnegie Mellon University (2004). *Creating and Managing Computer Security Incident Response Teams (CSIRTs).* Carnegie Mellon University 1996-2004. **https://www.first.org/resources/papers/conference2004/t1_01.pdf**.

Cichonski, Paul, Millar, Tom, Grance, Tim, y Scarfone, Karen (2021). *Computer Security Incident Handling Guide.* NIST. **https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf**.

Dufkova, Andrea (2020). *FIRST Site Visit Requirements and Assessment.* FIRST. **https://www.first.org/membership/site-visit-v3.1.pdf**.

Eguren, Enrique, Caraj, Marie (eds.) (2009). *Nuevo manual de protección para los defensores de derechos humanos.* Protection International. **https://www.protectioninternational.org/wp-content/uploads/2012/04/Nuevo_Manual_Proteccion.pdf**.

ENISA (2006). *Cómo crear un CSIRT paso a paso.* **https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-spanish**.

ENISA (2020). *How to set up CSIRT and SOC - Good Practice Guide*. **https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc**.

FIRST (2006). *CERT-in-a-Box.* GOVCERT.NL/NCSC. **https://www.first.org/resources/guides/cert-in-a-box.zip**.

FIRST (2019). *FIRST CSIRT Framework - Computer Security Incident Response Team (CSIRT)* Services Framework. **https://www.first.org/standards/frameworks/csirts/FIRST_CSIRT_Services_Framework_v2.1.0.pdf**.

Fondo de Población de las Naciones Unidas (2020). *Guía técnica de servicios remotos: Atención psicosocial especializada para sobrevivientes de violencia basada en género.* UNFPA. **https://lac.unfpa.org/sites/default/files/pub-pdf/unfpa_guiavbg_web_1.pdf**.

Haché, Alexandra (2021). *Modelos de líneas de Atención Feministas orientadas a las Violencias Machistas Digitales. Programa de Defensoras Digitales* (Digital Defenders Partnership). **https://www.digitaldefenders.org/modelos-de-lineas-de-atencion-feministas-orientadas-a-las-violencias-machistas-digitales/**.

Haché, Alexandra, y Alfama, Eva (2022). *Servicios y líneas de atención que dan apoyo a personas que enfrentan violencias machistas digitales: Mapeo internacional de los modelos de atención.* Fembloc. **https://fembloc.cat/archivos/recursos/6/implementation-studydef.pdf**.

Higson Smith, Craig, Ó Cluanaigh, Daniel, Ravi, Ali G., Steudtner, Peter (2016). *Holistic Security - A Strategy Manual for Human Rights Defenders. Tactical Technology Collective.* **https://holistic-security.tacticaltech.org/**.

INHOPE (2020). *Establishing a hotline guide,* INHOPE, **https://inhope.org/EN/hotline-guide**.

International Federation of Red Cross (2020) *Hotline in a Box.* IFRC. **https://www.communityengagementhub.org/wp-content/uploads/sites/2/2020/03/200325_Full-toolkit.pdf**.

Organización Internacional para las Migraciones (2007). *The IOM Handbook on Direct Assistance for Victims of Trafficking.* OIM. **https://publications.iom.int/system/files/pdf/iom_handbook_assistance.pdf**.

Kral, Patrick (2021). *Incident Handler's Handbook.* SANS Institute. **https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901**.

Maxigas (2014). *Hacklabs and Hackerspaces:* Shared Machine Workshops. Technological Sovereignty Vol. 1. Passerelles 11. **https://www.coredem.info/rubrique48.html**.

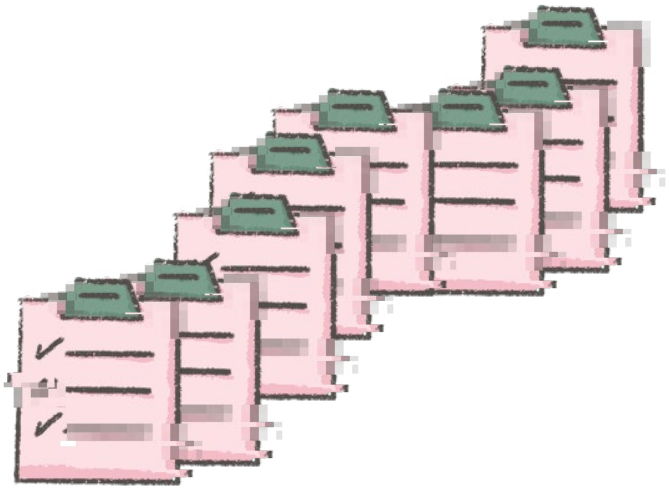
Stratten, Kate, y Ainslie, Robert (2003). *Field Guide: Setting Up a Hotline. Field Guide.* Johns Hopkins Bloomberg School of Public Health - Center for Communication Programs. **https://pdf.usaid.gov/pdf_docs/PNACU541.pdf**.

Tsunga, Arnold (ed.) (2007). *Protection Handbook for Human Rights Defenders. Front Line Defenders*. **https://www.frontlinedefenders.org/fr/file/1671/download?token=XHaqzSCK**.

Van der Heide, Martijn (2017). *Establishing a CSIRT. ThaiCERT, ETDA.* **https://www.thaicert.or.th/downloads/files/Establishing_a_CSIRT_en.pdf**.

West-Brown, Moira J., Stikvoort, Don, Kossakowski, Klaus-Peter, Killcrece, Georgia, Ruefle, Robin, y Zajicek, Mark (2003). *Handbook for Computer Security Incident Response Teams (CSIRTs).* Carnegie Mellon University. **https://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf**.

Zimmerman, Carson (2014). *Ten Strategies of a World-Class Cybersecurity Operations Center.* MITRE. **https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf**.



Plantillas

Plantilla de marco de trabajo

[Nombre de la organización]

1. Nuestro público

- ¿Quiénes son las beneficiarias de su LASDSC? Especificar actividad, ámbito, sexo, edad, etc. Cuanto más precisa sea la definición del público, mayor será la capacidad de identificar sus necesidades y aumentar la calidad del servicio prestado.
- ¿Cuál es el ámbito geográfico de su público?
- ¿Existen otras LASDSC que presten servicios al mismo público en su región? En tal caso, ¿qué necesidades no atendidas cubrirá su LASDSC?

2. Las necesidades de nuestro público

Si deciden, por ejemplo, apoyar a comunidades indígenas de una determinada región, se puede hacer un análisis FODA para analizar las características. Por ejemplo:

	Útil	**Dañino**
Interno	***Fortalezas*** Están muy bien organizadas y tienen acceso a una amplia variedad de recursos.	***Debilidades*** La estructura vertical centraliza la toma de decisiones.
Externo	***Oportunidades*** Muchas agencias de cooperación internacional están destinando fondos a comunidades indígenas.	***Amenazas*** Aumento de la criminalización de las comunidades indígenas.

Ahora intenten usar la misma tabla para sus beneficiarias:

	Útil	**Dañino**
Interno	***Fortalezas*** Describan las fortalezas de su público.	***Debilidades*** Describan las debilidades de su público.
Externo	***Oportunidades*** Describan las oportunidades de su público.	***Amenazas*** Describan las amenazas que afectan a su público.

Pueden complementar el marco FODA con un análisis PESTEL del contexto en el que se mueve su público.

Público	*Político*	*Economico*	*Sociocultural*	*Tecnológico*	*Ecológico*	*Legal*
Comunidades indígenas de X región	...	...	...	...	...	...

Matriz de amenazas

Probabilidad / Impacto	**Bajo**	**Medio**	**Alto**
Probable	...	...	...
Poco probable	...	...	...
Improbable	...	...	...

Inventario de amenazas

Completen una tabla para cada amenaza identificada en la matriz de amenazas.

Título	
Descripción *Breve caracterización de la amenaza.*	

Qué	**Objetivo**	**Atacante**	**Cómo**	**Dónde**
Los efectos que causaría la amenaza	*Qué o quién es el objetivo*	*¿Quién creen que está detrás de la amenaza?*	*Los medios por los que la amenaza puede llegar a materializarse*	*¿Cuáles son los espacios físicos en los que se puede manifestar la amenaza?*
...	...	...	...	...

3. Nuestra misión

¿Cuáles son los objetivos de la línea de ayuda? En la declaración de misión debe definirse el público al que se dirigen, la situación que se quiere mejorar y la forma en que piensan hacerlo, así como los servicios que prestará la línea de ayuda.

Nombre de la organización - Misión

Describan su misión aquí:
.....
.....
.....
.....

4. Diseño organizacional

- ¿Formará parte de una organización más grande o se trata de un proyecto independiente?
- ¿Será un equipo de personas voluntarias o se contratará al personal?
- ¿Cómo se financiará la LASDSC?

5. Servicios básicos

Tipo de servicio	Servicio	Requisitos
Reactivo	*Reposición de equipo*	*Acceso a financiación. Quizá podamos recuperar equipos antiguos para emergencias.*
Preventivo	*Formación presencial en seguridad digital*	*Es preciso encontrar personas que puedan impartir las formaciones en la zona donde se realizarán.*
...	...	...
...	...	...
...	...	...

6. Comunicación con su público

Decidan cómo se puede poner en contacto su público

Canal	Ventajas	Desventajas	Accesibilidad para nuestro público	¿Vamos a utilizarlo?
Formulario en el sitio web	*Fácil de instalar. Se puede cifrar.*	*Riesgo de spam.*	*Accesible*	*Sí*
Teléfono	*Todo el mundo puede acceder a un teléfono para llamarnos.*	*Las tarjetas SIM tienen que estar registradas con una ID.*	*Accesible*	*No*
...	...	...	...	...
...	...	...	...	...
...	...	...	...	...

Declaren su disponibilidad y tiempo de respuesta

Horario de atención:

- ¿Cómo se atenderán las solicitudes de apoyo fuera del horario de atención?
- ¿Cómo evitará la LASDSC el desgaste del equipo de asistencia?

Decidan cómo comunicarse con su público

- ¿El personal que responda las llamadas tendrá un seudónimo individual o utilizarán uno colectivo?
- ¿Lleva siempre una misma persona la comunicación con la persona implicada en un caso? Y si es compartida, ¿se mantiene la conversación siempre bajo el mismo seudónimo o se cambia con cada persona?
- ¿La LASDSC utilizará un tono informal o se mantendrá una distancia?

7. Políticas

Política	Descripción	Desarrollo e implementación	Responsable	Fecha
1.Política de gestión de la información	*Procedimientos para gestionar y proteger la información.*	Sí	...	...
2. Plan de respuesta a incidentes	*Hoja de ruta para implementar la capacidad de respuesta a incidentes de la LASDSC.*	*Sí*	...	...
3. Política de verificación	*Pasos para verificar a nuevas beneficiarias.*	Sí	...	...
4. Código de conducta	*Descripción del comportamiento que se espera de las operadoras.*	*Sí, pero en una segunda fase*	...	...
5. Procedimientos estándar de funcionamiento	*Pasos para responder las solicitudes, realizar derivaciones, etc.*	*Sí*	...	...
6. Política de financiación	...	...	...	...
7. ...	...	...	...	...

Plantilla de Código de conducta

[Nombre de la organización]

Código de conducta

Este código de conducta se aplica a todos los espacios de ***[Nombre de la organización],*** tanto si se trata de interacciones en línea como de espacios de trabajo presenciales, eventos asociados o reuniones sociales. El personal y las personas voluntarias son responsables de conocer los valores que defiende ***[Nombre de la organización]*** que se describen en este documento, y de respetar las normas que se citan a continuación.

La misión de ***[Nombre de la organización]*** es [descripción de la misión de la organización]. ***[Nombre de la organización]*** se compromete a proporcionar un entorno seguro y acogedor para llevar a cabo esta misión. En especial, queremos erradicar la vergüenza o el estigma que rodea los errores de seguridad digital o *hacking*, por lo que animamos a todas las personas implicadas a abordar las interacciones con una actitud abierta, de escucha y de apoyo y a implicarse de forma constructiva con las demás personas en todo momento.

Más concretamente, todas las partes de ***[Nombre de la organización]*** se comprometen a promover los siguientes valores:

> **Confidencialidad:** Trataremos toda la información que recibamos de forma confidencial y no la revelaremos a terceros sin consentimiento. Trataremos la información entrante de forma responsable y la protegeremos contra la divulgación involuntaria a partes no autorizadas. El grado de seguridad de los métodos de almacenamiento y transmisión de la información dentro o fuera de ***[Nombre de la organización]*** se adecuará a la sensibilidad de la misma. Invitamos a todo el personal y a las personas voluntarias a que lean la política de ***[Nombre de la organización]*** sobre cómo se debe clasificar, almacenar, compartir y destruir la información.
> Cualquier coordinación remota o iniciativa en línea se llevará a cabo a través de canales seguros que funcionen con software libre y de código abierto y, especialmente, si no están cifrados de extremo a extremo, serán gestionados y alojados por terceras partes de confianza, idealmente por la propia ***[Nombre de la organización]***. Se evitarán las herramientas comerciales o propietarias, especialmente si tienen un historial de violación de la privacidad.
> **Colaboración:** Tenemos un compromiso firme con el fomento de la solidaridad, la conexión, la cooperación y el sentido de comunidad en nuestros espacios.
> **Inclusividad:** Creemos en la importancia de la diversidad para favorecer la no discriminación, la libre expresión, la participación y la igualdad.
> **No-Hacer-Daño:** Somos conscientes de cómo nuestras acciones, comportamientos y formas de comunicación pueden tener un efecto positivo o negativo sobre las personas que nos rodean y tratamos de mitigarlo en la medida de lo posible. Somos conscientes de los factores que afectan nuestra propia situación de poder y reconocemos estas estructuras en los espacios de ***[Nombre de la organización]***. El objetivo de ***[Nombre de la organización]*** es ofrecer una experiencia libre de acoso para todas las personas, independientemente de su género, identidad y expresión de género, edad, orientación sexual, capacidad, apariencia física, tamaño corporal, raza, et-

nia, religión (o ausencia de la misma), elecciones, habilidades o nivel de conocimiento tecnológico. No toleramos el acoso en ninguna de sus formas. Cualquier persona que viole este código de conducta puede ser sancionada o expulsada de estos espacios a discreción de ***[Nombre de la organización]***.

Acoso

El acoso puede producirse en línea o de forma presencial. Ejemplos de comportamiento inaceptable:

1. Comentarios ofensivos que refuerzan las estructuras sociales de dominación o hacen alusión al género, la identidad y expresión de género, orientación sexual, discapacidad, enfermedad mental, neuro(a)tipicidad, apariencia física, tamaño corporal, edad, raza o religión.
2. Comentarios ofensivos y guerras de *flames* (publicaciones incendiarias sobre) sobre las elecciones de otras personas en cuanto a prácticas, destrezas, procedimientos y herramientas recomendadas.
3. Comentarios desagradables sobre las elecciones y prácticas de estilo de vida de una persona, entre otras las relacionadas con la alimentación, la salud, la crianza, las drogas y el empleo.
4. La utilización deliberada de un género inapropiado o el uso de nombres "muertos" (*deadnames*) o rechazados.
5. Imágenes o comportamientos sexuales gratuitos o fuera de lugar en espacios donde no son apropiados.
6. Contacto físico y contacto físico simulado (por ejemplo, descripciones textuales como "abrazo" o "caricia en la espalda") después de que se haya solicitado que se pare. Amenazas de violencia.
7. Incitación a la violencia hacia cualquier persona, lo que incluye animar a una persona a que se suicide o autolesione.
8. Intimidación deliberada.
9. Acosar o perseguir a alguien.
10. Usar fotos o videos para acosar, incluido el registro de la actividad en línea con fines de acoso.
11. Interrumpir de forma constante debates, charlas u otros eventos.
12. Atención sexual o contacto físico no deseados.
13. Conductas de contacto social inapropiado, como solicitar/asumir un nivel de intimidad inapropiado con otras personas.
14. Persistencia de una comunicación individual después de que se haya pedido que cese.
15. La divulgación deliberada de algún aspecto de la identidad de una persona sin su consentimiento (*outing*), excepto cuando sea necesario para proteger a personas vulnerables de abuso intencionado.
16. La publicación de comunicación privada no acosadora.
17. Publicar información privada de otra persona, como su dirección física o electrónica, sin permiso explícito.
18. Defender o fomentar cualquiera de las conductas anteriores.
19. Introducir alguna droga en la comida o bebida.
20. Violar la política de privacidad de un evento con el fin de generar atención negativa hacia una persona que participa.
21. Solicitar la ayuda de otras personas, ya sea presencial o en línea, para atacar a alguien. Priorizamos la seguridad de las personas marginadas frente a la comodidad de las privilegiadas.

Nuestro equipo no actuará ante denuncias por:

- Los ismos "inversos", como el "racismo inverso", el "sexismo inverso" y la "cisfobia".
- Comunicación razonable sobre límites, como: "déjame en paz", "vete" o "no voy a hablar contigo de esto".
- Comunicación en un "tono" que no te parece agradable.
- Críticas de comportamientos o suposiciones racistas, sexistas, cisexistas o de otro tipo.

NOTA:
Permitir que una persona abandone una conversación que le resulte incómoda y no seguir a quien haya pedido que se le deje sola. Si se tratan temas difíciles, que pueden avivar un trauma para las personas participantes, es importante no olvidarse de advertirlo para que estas puedan abandonar la conversación o prever estrategias para afrontarla.

Denuncias

Si estás sufriendo acoso, observas que otra persona está siendo acosada o tienes cualquier otra preocupación, notifícanoslo enviando un correo electrónico a ***[dirección de correo electrónico específica]***. Actualmente, hay ***[n.]*** personas que reciben estos correos electrónicos: ***[nombres]***. Las denuncias son confidenciales. No se pedirá que tomes ninguna medida que te produzca inseguridad.

Este código de conducta se aplica a los espacios de ***[Nombre de la organización]***, pero si una persona que participa en ***[Nombre de la organización]*** te acosa fuera de nuestros espacios, también queremos saberlo. Nos tomaremos en serio todas las denuncias de acoso de buena fe (tanto el acoso fuera de nuestros espacios como el que haya tenido lugar en cualquier momento).

El equipo de respuesta se pondrá en contacto con la persona acusada para informarle del proceso y ofrecerle la oportunidad de responder. El equipo de respuesta se reserva el derecho de excluir a personas de ***[Nombre de la organización]*** en función de su comportamiento pasado, lo que incluye el comportamiento fuera de los espacios de ***[Nombre de la organización]***. Respetaremos las solicitudes de confidencialidad con el fin de proteger a las víctimas de abusos. Queda a nuestra discreción la decisión de nombrar públicamente a una persona sobre la que hayamos recibido denuncias de acoso o de advertir en privado a terceros sobre ella si creemos que hacerlo aumentará la seguridad de las socias o de quienes forman parte de ***[Nombre de la organización]***. No nombraremos a las víctimas de acoso sin su consentimiento expreso.

El acoso y otras violaciones del código de conducta merman el valor de nuestra comunidad. Queremos que te sientas a gusto en ella, ya que gracias a gente como tú es un lugar mejor. Si la persona que te acosa forma parte del equipo de respuesta o de la dirección de ***[Nombre de la organización]***, se apartará de la gestión de tu incidente. Responderemos tan pronto como podamos.

Consecuencias

Se espera que cualquier integrante del personal o del voluntariado a quien se le pida que cese un comportamiento de acoso lo haga inmediatamente. Si alguien en ***[Nombre de la organización]*** incurre en un patrón de acoso, el equipo de respuesta puede tomar las medidas que considere oportunas, que pueden incluir el despido o la denuncia pública.

Licencia

Plan de respuesta a incidentes

[Nombre de la organización]

Plan de respuesta a incidentes

Este proceso describe la forma en que ***[Nombre de la Organización]*** recibe y responde a incidentes de seguridad informática. El proceso incluye la forma en que los incidentes se asignan, analizan, gestionan, elevan, cierran y revisan para obtener aprendizajes.

Recepción y asignación de incidentes

Cada vez que se recibe un incidente, la persona que lo gestiona es la responsable de proporcionar una respuesta inicial y garantizar el seguimiento del mismo. Esta primera respuesta debe proporcionarse lo antes posible y siempre debe producirse dentro de ***[plazo definido en el acuerdo de nivel de servicio de la LASDSC]***.

La persona designada para acompañar el caso es la responsable del análisis y la respuesta al incidente. Los criterios para decidir quién acompaña el caso deben tener en cuenta:

- Prioridad del caso.
- Idioma del caso / idiomas hablados por las gestoras de incidentes.
- Carga de casos de las gestoras de incidentes.
- Ubicación geográfica de la persona beneficiaria / zona horaria.
- Conocimientos necesarios para resolver el incidente.

Las personas responsables de cada turno se encargan de equilibrar la carga de trabajo dentro de las oficinas y entre ellas. Si lo precisa, una gestora puede solicitar que un caso que esté acompañando se transfiera a otra persona que pueda tener más herramientas para atenderlo. Esto debe hacerse con el acuerdo de ambas. Si es necesario, la persona beneficiaria también debe ser informada del cambio.

Asignación de prioridades

La prioridad del caso es un valor que se asigna a cada caso. Las prioridades ayudan a las personas que acompañan los casos y, en general, a la dirección de la LASDSC a asignar una cantidad adecuada de recursos a cada caso. También definen el orden en que deben resolverse los mismos. La prioridad refleja la respuesta organizativa necesaria para cada solicitud.

Entre las variables que se tienen en cuenta a la hora de priorizar, el impacto y la urgencia son las más relevantes

1. Impacto para la parte beneficiaria

En los casos en los que la persona beneficiaria está en peligro físico o digital y las consecuencias de no actuar pueden ser graves, deben ser abordados teniendo en cuenta las posibles consecuencias y efectos del problema y la solución a plantear. Existen tres categorías para definir el impacto de un caso: alto, moderado y bajo.

Para establecer el impacto de un caso, pueden consultar la siguiente tabla orientativa:

Categoría	Descripción
Alto (A)	- Una persona ha resultado herida o corre riesgo de resultar herida. - La persona beneficiaria está ante una situación reactiva/peligrosa. - Existe un alto riesgo de exposición de información sensible. - Es probable que la información personal de varias beneficiarias se vea expuesta. - Si la situación no se gestiona adecuadamente, puede dañarse la reputación de la línea de atención. - La persona beneficiaria puede ser alguien de perfil alto.
Medio (M)	- Las consecuencias del incidente pueden definirse como un valor intermedio, entre bajo y alto.
Bajo (B)	- El objetivo del caso es evitar un futuro incidente de seguridad para la organización. El asesoramiento brindado no pone a la persona beneficiaria en riesgo físico inminente.

2. Impacto para la LASDSC

A veces los casos pueden tener un impacto sobre la línea de atención y su reputación. Estos deben tratarse con especial cuidado, implicando al equipo directivo en su resolución.

3. Urgencia

Se define como la medida de retraso que se puede tolerar y la rapidez con la que se requiere una solución. Los casos pueden clasificarse como muy urgentes, moderadamente urgentes y no urgentes, depende de varios factores, entre ellos los distintos factores de tiempo y el nivel de amenaza si no se actúa en un plazo determinado.

Para establecer la prioridad del caso, quienes gestionan los incidentes también deben tener en cuenta lo que diga la persona beneficiaria cuando se abre el caso. A veces especifican que el caso es urgente por un motivo concreto. Para establecer la urgencia del caso, ofrecemos a continuación una tabla orientativa:

Categoría	Descripción
Alta (A)	- Las consecuencias causadas por el incidente aumentan rápidamente con el paso del tiempo. - Se puede evitar que un incidente menor se convierta en uno mayor si se actúa inmediatamente. - El caso se abrió de forma reactiva, por una beneficiaria que buscaba ayuda inmediata. - ¿Es un DDoS? ¿Se está produciendo una filtración de datos sostenida en el tiempo?
Media (M)	- Las consecuencias causadas por el incidente aumentan lentamente con el tiempo.
Baja (B)	- Las consecuencias de no resolver el caso no aumentan con el tiempo. - El objetivo del caso es evitar un futuro incidente de seguridad para la organización.

4. Prioridad

Mediante la combinación de los factores mencionados (urgencia e impacto), la persona que está gestionando el incidente puede evaluar la correspondiente prioridad del caso. La siguiente tabla resume la prioridad:

		Impacto		
		Alto	Medio	Bajo
Urgencia	Alto	1	2	3
	Medio	2	3	4
	Bajo	3	4	5

NOTA:
*Si existe alguna duda sobre la urgencia o el impacto de un caso, siempre es mejor pecar de prudencia y no correr ningún riesgo.**

Como norma general, si un caso tiene una prioridad mayor, también tiene un impacto relevante para la línea de atención y para la persona beneficiaria. Hay que tener en cuenta que, independientemente de la prioridad del caso, si la persona que gestiona el incidente no está segura del consejo que debe dar, debe solicitar el apoyo de sus compañeras.

Ciclo de vida de la respuesta a incidentes

Lo que viene a continuación es nuestro flujo de trabajo de respuesta a incidentes. Ofrece una visión general de cómo deben gestionarse los incidentes de seguridad digital. No contiene consejos sobre cómo abordar incidentes específicos. Para consejos específicos sobre cómo gestionar distintos tipos de incidentes, véase nuestra documentación de procedimientos.

El ciclo de vida de respuesta a incidentes que ha seguido la línea de atención está basado en: **Paul Cichonski, Tom Millar, Tim Grance, Karen Scarfone, Computer Security Incident Handling Guide, NIST, 2021. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.**

Cuando una organización se pone en contacto con nuestra LASDSC para solicitar apoyo preventivo, generalmente se está **preparando** y está ajustando sus prácticas para evitar que se produzcan incidentes de seguridad digital. Este es el escenario ideal, en el que ayudamos a nuestras beneficiarias a mitigar el riesgo de que su seguridad o sus datos se vean afectados.

A veces, la solicitud de la beneficiaria es que se investigue un posible incidente o intento de incidente. Este tipo de informes no cuentan con pruebas claras de que ya se haya producido un incidente, por lo que requieren una investigación inicial para verificar el informe y confirmar si ya se ha producido un incidente o no. Esta fase se denomina **detección** y la gestora puede requerir más pruebas para su investigación hasta que quede claro que el suceso realmente ha puesto en peligro la seguridad de la beneficiaria y que no se trata de un suceso sin consecuencias. Nuestra documentación de procedimientos debe ayudar a quien acompaña el caso a entender qué pruebas o información son útiles para investigar los distintos tipos de incidentes. Este tipo de casos normalmente son de urgencia media o alta, especialmente cuando aún se está determinando si se ha producido un incidente o no.

Sin embargo, a menudo las personas beneficiarias se ponen en contacto con nuestra línea de atención cuando ya se ha producido un incidente. Es decir, que ya se han producido una o varias agresiones que han dañado o intentan dañar intencionadamente el sistema, la red o los datos de la persona beneficiaria. Algunos ejemplos son: indisponibilidad del sistema, fuga de datos, secuestro del dispositivo, exposición de la cuenta, etc. Por lo tanto, normalmente damos prioridad a la **contención** de ese incidente para evitar que el daño se extienda a otras partes.

Las acciones que solemos adoptar para **contener los incidentes** incluyen: solicitar a una plataforma en línea que suspenda una cuenta expuesta, aislar de la red un sistema expuesto, suspender un sitio web desfigurado, eliminar datos que se están filtrando, etc. En la mayoría de los casos, la contención debe ser rápida y hay que priorizarla. En otros casos, dependeremos de las acciones de la persona beneficiaria para retirar su sistema de la red o aislarlo mientras proporcionamos las instrucciones técnicas a través de comunicaciones remotas. La urgencia de estos casos suele ser alta cuando se trata de contener un incidente que se está produciendo.

Cuando se consigue la contención, normalmente es importante que quien acompaña el caso dedique algún tiempo a analizar la causa que ha originado el problema. Esto suele dar lugar a una investigación que por lo general tiene lugar en la fase de **detección y análisis**. En función de la categoría del caso, se pueden solicitar pruebas adicionales a la persona beneficiaria para realizar el **análisis**, como el origen del correo electrónico malicioso recibido hace poco, el enlace para descargar una aplicación maliciosa, capturas de pantalla de las alertas antivirus, etc. El objetivo es determinar si se debe tomar alguna medida más para garantizar que la recuperación con respecto al incidente es plena. De nuevo, la persona que gestiona el caso debe consultar nuestra documentación de procedimiento para saber qué otra información puede ser útil para realizar su análisis.

La **erradicación** consiste en limpiar los sistemas expuestos para garantizar una recuperación plena. Puede ser tan sencillo como instalar y ejecutar una aplicación antivirus o, en algunos casos, puede requerir instalar de nuevo el sistema. Sin embargo, en todos los casos, es fundamental averiguar y documentar qué ha dejado el ente atacante (si es que ha dejado algo) y limpiarlo. Esto sirve para vigilar la posible reaparición del ataque y para detectar otros ataques similares contra otros sistemas o personas beneficiarias. En el caso de sistemas donde no es posible una nueva instalación o donde no se puede restablecer la configuración de fábrica, cabe eliminar de forma manual los artefactos del ente atacante identificados en la fase de análisis: véanse las tareas de inicio o cron para relanzar una puerta trasera. En casos como los ataques DDoS, la **erradicación** no es posible porque en estos incidentes el ataque no deja ningún artefacto y su origen está tan distribuido que derribar cada *host* implicado en el ataque no es posible ni razonable. Sin embargo, en los casos en los que la infraestructura del ente atacante no está distribuida, el desmantelamiento de esta infraestructura maliciosa debe considerarse parte de la fase de erradicación. Denunciar una cuenta que esté filtrando información o suspender una dirección de correo electrónico que esté enviando correos de *phishing* también podría considerarse **erradicación**. La erradicación normalmente no suele ser urgente, ya que la amenaza en general ya debería haberse contenido en esta fase. Sin embargo, si el sistema sigue vivo o conectado (según la preferencia de la persona propietaria) y el análisis ha descubierto artefactos que permiten que el ataque reaparezca pronto o inmediatamente, hay que asignarle al caso una urgencia alta.

La distinción entre la fase de recuperación y la de erradicación no siempre es clara, ya que la recuperación viene tras erradicar el artefacto del ente atacante: por ejemplo, cuando se elimina la dirección de correo electrónico o el número de teléfono de quien ha hackeado la cuenta y se asocia de nuevo a los datos legítimos o cuando se utiliza un antivirus para limpiar un gusano no persistente. Sin embargo, para garantizar la recuperación es importante, en algunos casos, vigilar cualquier posibilidad de reaparición del ente atacante. Esta tarea es especialmente importante cuando descubrimos que el ataque está muy focalizado y la amenaza es persistente. En estos casos, los entes atacantes no dudarán en volver a atacar utilizando la misma vulnerabilidad/debilidad o buscando otras. Según lo factible que sea hacerlo, se puede ayudar a una persona beneficiaria a monitorizar cualquiera de los artefactos que ya se han encontrado y eliminado en la fase de erradicación.

La labor **posterior al incidente** consiste en actividades preventivas que se pueden llevar a cabo tras el ataque. Puede tratarse de formación, refuerzo del sistema, pruebas de penetración, una auditoría de seguridad y una evaluación de la organización de la persona beneficiaria, entre otras cosas. Sin embargo, parte de este trabajo preventivo podría realizarse en una fase anterior del incidente para garantizar también una recuperación plena. Por ejemplo, una persona beneficiaria cuya cuenta haya sido hackeada podría recibir ayuda para crear una nueva dirección de correo electrónico protegida con una contraseña fuerte y una autentificación de dos factores para poder recuperar su cuenta. En casos de exposición del sistema, se podría realizar un escaneo de vulnerabilidad en el sistema para eliminar cualquier vulnerabilidad que permita nuevos ataques antes de que este sistema vuelva a estar operativo. En los casos de acoso, la investigación de inteligencia de código abierto podría ayudar a la víctima a recuperarse de un acoso anterior e identificar cualquier información disponible en línea que pudiera ser utilizada de nuevo por el ente atacante. La actividad posterior al incidente necesaria para recuperarse del mismo ¡no debe figurar nunca con una urgencia baja asignada!

Consideraciones importantes

A la hora de responder a las solicitudes se debe tener en cuenta lo siguiente:

- Tras la recepción de un caso, además de la respuesta automática enviada por el sistema de gestión de tickets, la persona que esté de turno debe responder personalmente a la persona solicitante, explicándole que se encargarán del caso y poniéndose a su disposición para cualquier cuestión que pueda surgir.
- El proceso de verificación de una nueva persona beneficiaria puede llevar cierto tiempo. Mientras se lleva a cabo este proceso, la acompañante del caso debe comenzar a trabajar en la solución, teniendo en cuenta que hasta que no se verifique a la beneficiaria, se debe tener un cuidado especial en cuanto a la información que se comparte y a las acciones que se llevan a cabo, ya que aún no se ha confirmado el vínculo de confianza.
- Cuando busquen soluciones para los casos, tengan siempre en cuenta las siguientes recomendaciones:
  - Busquen documentación de procedimiento relacionada.
  - Deriven o recurran a otras organizaciones o personas afines para casos específicos.
  - Consideren la posibilidad de acudir a CiviCERT.
  - En caso de que se encuentren en un callejón sin salida, eleven siempre el caso y consúltenlo con la dirección.

Razones para cerrar un caso

A la hora de cerrar un caso, la persona que lo gestiona debe registrar el motivo por el que lo cierra. Las opciones posibles son:

- **Resuelto con éxito:** Se ha logrado cumplir el objetivo del caso.
- **Falta de respuesta de la persona solicitante:** La persona beneficiaria no ha respondido después de varias comunicaciones.
- **Futura mejora:** El objetivo del caso no se ha cumplido en su totalidad y se llevarán a cabo otras acciones en el futuro.
- **Solución fallida:** No se ha logrado cumplir el objetivo del caso.
- **Petición de la persona solicitante:** La persona solicitante pidió explícitamente que el caso se cierre.
- **Cancelación interna del caso:** El caso fue cancelado a petición de una persona del equipo interno.

Un caso solo debe cerrarse por falta de respuesta de la persona beneficiaria si esa falta de respuesta nos impide responder a la incidencia. Si la persona que está gestionando la incidencia ha cumplido los requisitos para concluir el caso, este debe etiquetarse como resuelto con éxito, independientemente de que tengamos o no noticias de la persona beneficiaria.

Política de gestión de la información

[Nombre de la organización]

Política de gestión de la información

1. Clasificación de la información

[Nombre de la organización] apoya el protocolo de semáforo para el intercambio de información.

Descripción de la clasificación de datos

- **PÚBLICA** – Esta información se considera no sensible (es decir, que no incluye datos personales ni detalles sobre colaboraciones con terceras partes y procedimientos internos) y puede transmitirse a cualquier persona en cualquier contexto. La información está destinada al consumo público. Es posible que ya se haya informado sobre ella o que esté disponible para ello.

- **CONFIDENCIAL** – La información con la etiqueta de confidencial puede compartirse con otros equipos de ***[Nombre de la organización]***, así como con terceras partes de confianza en función del principio de la necesidad de saber ("*need-to-know*"), es decir, únicamente si para abordar un caso específico esa información es imprescindible. Por defecto, la información solo se comparte entre el personal de ***[Nombre de la organización]***. No se debe dar nunca por hecho que la información se comparte con terceras partes: de hecho, este tipo de información solo debe compartirse con terceras partes bajo el principio de la necesidad de saber y en tanto en cuanto hayan firmado un acuerdo de no divulgación que incluya unas normas mínimas sobre el almacenamiento y la conservación de datos ajustadas a la Política de conservación de ***[Nombre de la organización]*** (véase más abajo).

- **RESTRINGIDA:** ***[grupo / entidad / lista de personas]*** – Toda información con la etiqueta de restringida debe incluir también un grupo, entidad o lista de personas que no tengan restringido el acceso a la información. Cuando el acceso a la información está restringido a ciertos grupos o entidades, la pertenencia de cualquier persona a ese grupo o entidad implica que esa persona tiene acceso a la información. La información restringida también puede compartirse con terceras partes bajo el principio de necesidad de saber. De modo que, en los casos de información con la etiqueta "RESTRINGIDA: Equipo técnico de ***[Nombre de organización]***", las otras partes pueden ser la persona beneficiaria, además de otra tercera parte que sea preciso incluir para poder resolver el caso. Alguna información es tan sensible que solo debe compartirse con personas que necesiten absolutamente conocerla. En ese caso, se etiquetará como "RESTRINGIDA: ***[lista de personas]***". Esta información nunca se comparte con los grupos, por lo que la pertenencia a un grupo nunca concede acceso a esta clasificación de la información. Cuando se envía un correo electrónico, se considera personas que "necesitan saber" únicamente a las personas destinatarias y en ningún caso se debe compartir la información más allá.

Color	Clasificación	Alcance	Ejemplos
ROJO	RESTRINGIDA [lista de personas]	Personas citadas.	· Solicitudes de carácter jurídico. · Cuestiones de confianza.
ÁMBAR	RESTRINGIDA [entidad]	Integrante de [entidad] y terceras partes que necesitan saber.	· Solicitudes de personas beneficiarias. · Datos del historial del caso (que pueden incluir datos personales necesarios para la prestación de servicios). · Contactos personales (si es necesario y está justificado por una solicitud de integrantes de la entidad y de terceras partes). · Documentación sobre infraestructura interna. · Documentación sobre procesos internos.
VERDE	CONFIDENCIAL	***[Nombre de la organización]*** integrantes; terceras partes que necesitan saber.	· Inteligencia sobre amenazas a la sociedad civil. · Documentación sobre elevaciones y procedimientos.
BLANCO	PÚBLICA	Toda.	· Recomendaciones de seguridad general. · Entradas de blog. · Contenido de sitio web. · Entradas de redes sociales .

2. Protección de la información

- La información pública se puede difundir ampliamente, ya sea mediante boletines informativos, contenidos de sitios web, publicaciones en redes sociales, información en plataformas públicas de intercambio de información sobre *malware*, etc. La infraestructura de ***[Nombre de la organización]*** que aloja la información pública está reforzada y protegida contra el riesgo de daño a su integridad. Toda la información pública está respaldada con una copia de seguridad para evitar que se pierda.
- La información confidencial se almacena en plataformas a las que solo puede acceder el personal de ***[Nombre de la organización]*** y que pueden compartirse con terceras partes bajo el principio de la necesidad de saber. El acceso a estas plataformas está protegido por contraseña y requiere una autentificación de dos factores siempre que es posible. Este tipo de información también se almacena en dispositivos de trabajo con cifrado de disco completo. Este tipo de información solo se transfiere a través de canales de comunicación cifrados de extremo a extremo.
- **La información restringida**

  La información restringida a equipos específicos de *[Nombre de la organización]* solo se almacena en plataformas protegidas con contraseña y en dispositivos de trabajo con cifrado de disco completo. Este tipo de información solo se transfiere a través de canales de comunicación cifrados de extremo a extremo.

  La información restringida a personas solo se almacena en plataformas protegidas con contraseña y solo se transfiere a través de canales de comunicación cifrados de extremo a extremo.

Las claves privadas GPG del personal solo se almacenan en sus dispositivos portátiles con cifrado de disco completo o en soportes de almacenamiento externo totalmente cifrados.

Las medidas de seguridad establecidas para la protección de la información son normas de mínimos y, como están en constante evolución, pueden cambiar en el futuro.

3. Difusión de la información

Información que no puede ser compartida:

- La información entrante restringida a personas específicas no se compartirá más allá de las personas destinatarias citadas.

Limitaciones de esta política:

- La información puede ser compartida en cumplimiento de las obligaciones jurídicas nacionales e internacionales, incluida la respuesta a solicitudes de las autoridades policiales que obliguen a ***[Nombre de la organización]*** a presentar sus registros. ***[Nombre de la organización]*** se opondrá firmemente a los requerimientos judiciales u otras solicitudes que infrinjan los derechos humanos y empleará todos los medios a su alcance para proteger a su personal, personas y entidades beneficiarias y socias.

4. Acceso a la información

Los requerimientos judiciales por parte de las autoridades, las comunicaciones sobre cuestiones de confianza y otra información crítica pueden tener la etiqueta de información RESTRINGIDA, permitiendo el acceso solo a personas a nivel individual y únicamente en función de la necesidad de saber, hasta que sea posible rebajar el nivel de confidencialidad de esta información..

Cambiar la clasificación de los datos

La información que reciba la etiqueta de CONFIDENCIAL solo puede hacerse pública tras eliminar toda la información sensible o con la autorización explícita de las personas y grupos mencionados en dicha información. Si la información tiene la clasificación de confidencial solo por exclusividad de los derechos de publicación, pasará automáticamente a tener la clasificación de pública en el momento en que se publique.

5. Cooperación con otros equipos

Esta política define el proceso que sigue ***[Nombre de la organización]*** para cooperar formal o informalmente con otros CERT y equipos de respuesta de seguridad digital para la sociedad civil.

- ***[Nombre de la organización]*** puede compartir información con la etiqueta de "PÚBLICA" en cualquier foro al que tenga acceso un CERT o equipo de respuesta de seguridad digital para la sociedad civil.
- Si ***[Nombre de la organización]*** considera que la mejor acción a favor de una persona beneficiaria es colaborar con otro CERT específico o con un equipo de respuesta de seguridad digital para la sociedad civil, esas comunicaciones y los datos asociados deben clasificarse bajo las etiquetas de "CONFIDENCIAL" o "RESTRINGIDA: ***[lista de entidades]***" (véase "Clasificación de la información" arriba).
- En estos casos, ***[Nombre de la organización]*** solicitará el permiso de la persona beneficiaria para tratar de resolver su caso a través de los servicios de otro CERT o equipo de respuesta de seguridad digital para la sociedad civil.

  En algunos casos, ***[Nombre de la organización]*** no necesitará la autorización de la persona beneficiaria, pues dicha autorización puede darse por supuesta, por ejemplo:

    - Si la persona beneficiaria ha encargado al CERT o al equipo de respuesta de seguridad digital para la sociedad civil que retire un host de contenido de phishing (conviene tener en cuenta que, antes de proceder a la resolución de estos casos, deben seguirse primero nuestros procesos sobre coordinación de inteligencia sobre amenazas y buscar las acciones más beneficiosas para el mayor número de partes interesadas en tales circunstancias);
    - Recuperación o desactivación de la cuenta (siempre que se haya verificado a la persona beneficiaria) con el CERT de la plataforma implicada;
    - Una queja por cierre, si ese cierre ha afectado al público en general.
- Circunstancias en las que se requiere obligatoriamente un permiso de la persona beneficiaria:
    - Desactivar un servidor de comando y control (C&C);
    - Análisis de malware, especialmente cuando se va a analizar un dispositivo;
    - Sortear la censura.

6. Conservación de registros

Toda la información compartida dentro de [Nombre de la organización] se almacena en los propios servidores de [Nombre de la organización], a los que se aplica la siguiente política:

Política de conservación

Toda la información de la infraestructura de ***[Nombre de la organización]***, incluida la información sobre amenazas, las solicitudes de las personas beneficiarias y entidades socias y la documentación interna, se almacena durante el tiempo que sea necesario en los servidores de ***[Nombre de la organización]*** con el fin de compartir la información y prestar los servicios, así como para cumplir con las obligaciones legales nacionales e internacionales, incluida la prevención de delitos penales y el curso de demandas civiles.

Toda la información de la infraestructura de ***[Nombre de la organización]***, excepto la información pública que no es sensible y no incluye ningún dato personal, se almacena en plataformas protegidas con contraseña y en dispositivos de trabajo con cifrado de disco completo. Este tipo de información solo se envía a través de canales de comunicación cifrados de extremo a extremo. Estas son las normas de mínimos vigentes, que, debido a que están en constante evolución, pueden cambiar en el futuro.

Política de filtración de datos

En caso de que se produzca una filtración de datos personales que pueda suponer un riesgo para los derechos y libertades de las personas a las que se refieren los datos, ***[Nombre de la organización]*** notificará a estas personas y a la autoridad de supervisión competente sin demora indebida y siempre que sea posible, a más tardar 72 horas después de haber tenido conocimiento de la filtración, de conformidad con el Reglamento General de Protección de Datos de la UE.

A la hora de tratar filtraciones de seguridad de datos, ***[Nombre de la organización]*** adoptará medidas para mitigar los daños, investigar, llevar a cabo medidas correctivas y cumplir con los requisitos normativos en materia de seguridad de la información.

7. Proceso de destrucción de datos

Documentos físicos

La impresión de documentos debe limitarse al mínimo. Los documentos impresos deben almacenarse únicamente el tiempo necesario y se recomienda no cruzar fronteras con documentos impresos confidenciales o de uso restringido.

Los documentos en papel que contengan información CONFIDENCIAL deben ser destruidos en una trituradora de tiras o de corte transversal, mientras que cualquier otro documento físico que contenga información RESTRINGIDA debe ser destruido con una trituradora de corte transversal.

Dispositivos de almacenamiento

Los discos duros, las memorias USB y otros dispositivos de almacenamiento portátiles que contengan información CONFIDENCIAL o RESTRINGIDA deben borrarse de forma segura con una única pasada del proceso de borrado: datos aleatorios (/dev/urandom) antes de eliminarlos. Los CD de una sola escritura deben romperse en pedazos o destruirse en la trituradora antes de tirarlos.

Datos digitales

Los archivos digitales que contengan información CONFIDENCIAL se pueden borrar directamente, mientras que para los datos RESTRINGIDOS se debe realizar como mínimo un proceso de borrado sobre el archivo.

8. Uso adecuado de los dispositivos de trabajo

Todo el personal de [Nombre de la organización] se asegura de que los dispositivos con los que acceden a información de [Nombre de la organización] estén protegidos con cifrado de disco completo y se utilicen con buen criterio, con actualizaciones periódicas del sistema y del software y otras medidas para evitar infecciones o accesos no autorizados al sistema y a las cuentas.

9. Política de comunicaciones y PGP de [Nombre de la organización]

La información "RESTRINGIDA" solo debe compartirse entre el personal de ***[Nombre de la organización]*** a través de canales con un alto grado de cifrado, como correos electrónicos cifrados con PGP, Signal o similares.

[Nombre de la organización] apoya las comunicaciones cifradas con PGP y se comunica a través de un canal cifrado.

Todo el personal de ***[Nombre de la organización]*** está obligado a utilizar PGP/GnuPG para cifrar todas las comunicaciones por correo electrónico con:

- otras personas del equipo
- terceras partes, cuando intercambien información confidencial y restringida

Se recomienda que los pares de claves PGP utilizados para comunicarse entre el personal de ***[Nombre de la organización]*** y con terceras partes tengan la siguiente configuración:

- Algoritmo: RSA
- Longitud de clave: 4096
- Fecha de caducidad: 5 años
- Clave privada protegida por una contraseña fuerte, compuesta por al menos 20 caracteres, incluyendo letras minúsculas y mayúsculas, números y símbolos o una frase de contraseña creada con el método *diceware*, con al menos 6 palabras.

En caso de que un dispositivo que contenga una clave privada PGP sea robado o de que un par de claves PGP se vea expuesto de otro modo, el par de claves será revocado lo antes posible y se notificará a la dirección de ***[Nombre de la organización]***.

Proceso de verificación

[Nombre de la organización]

Proceso de verificación

Objetivo de la verificación

El objetivo de verificar a las personas beneficiarias es tratar de reducir el riesgo para ***[Nombre de la organización]*** y para las personas usuarias en situación de riesgo.

Algunos de los riesgos que mitiga la verificación son el riesgo para ***[Nombre de la organización]*** de que su reputación se vea perjudicada por trabajar con organizaciones que no defienden los derechos humanos básicos o que son controvertidas por cualquier otro motivo. También existe el riesgo de que entes atacantes nos manipulen para que divulguemos información o para que permitamos que entren en nuestras plataformas, lo que les permitiría perpetrar ataques eficaces contra nuestras actividades. Asimismo, se corre el riesgo de que consuman nuestros recursos en incidentes falsos, privando así a personas y organizaciones que realmente necesitan nuestra ayuda de esa posibilidad.

La verificación es un ejercicio de diligencia debida con las personas a las que asistimos para asegurarnos de que realmente forman parte del público al que nos dirigimos.

Para asegurarnos de que este proceso de verificación queda debidamente registrado, todas las comunicaciones requeridas para completar el proceso de verificación se graban en orden cronológico en el historial del caso.

Proceso de verificación de *[Nombre de la organización]*

El proceso utilizado para verificar a todas las nuevas beneficiarias consta de los siguientes pasos:

1. Evaluación inicial
2. Identificar/contactar a las posibles personas/entidades verificadoras
3. Evaluación de respuestas
4. Validación y registro

1. Evaluación inicial

Se puede realizar una investigación preliminar a través de fuentes de información como Google, Wikipedia, el propio sitio web de la persona solicitante, *Whois*, servidores de claves PGP, etc. para comprobar la veracidad de la organización y la persona en cuestión. Ninguna de estas fuentes por sí sola debe considerarse fiable, pero su combinación permite hacerse una idea de la legitimidad de la organización/persona.

2. Identificar/contactar a posibles verificadoras

El siguiente paso es identificar a posibles verificadoras. Es preciso localizar a una persona que ya conozcamos y en quien confiemos y que esté dispuesta a avalar a la posible nueva beneficiaria.

Un buen punto de partida es buscar en el sitio web de la organización, especialmente en secciones donde figuran las personas que integran su junta directiva, que suelen ser personas de alto perfil en el ámbito de las ONG y a menudo conocidas por el personal de ***[Nombre de la organización]*** o por sus organizaciones socias, por lo que es una forma excelente de localizar a posibles avalistas.

3. Evaluación de las respuestas

Lo que intentamos comprobar es que la persona beneficiaria es quien dice ser, y que actúa de forma racional, segura y respetuosa hacia otras personas. Es importante que la beneficiaria esté en condiciones de respetar la reputación de ***[Nombre de la organización]*** si queremos que la organización participe prestando su ayuda. En gran medida, esto es lo que intentamos evaluar.

No se trata de una decisión definitiva sobre la "idoneidad", ya que la naturaleza de las relaciones de confianza siempre es un tanto subjetiva. Sin embargo, como norma general, podemos estimar que si alguien en quien confiamos implícitamente avala a una nueva beneficiaria, podemos considerar que está verificada. Si no logramos encontrar a nadie en quien confiemos implícitamente, para poder dar el visto bueno al proceso de verificación será necesario que dos personas conocidas de cuya reputación nos fiemos avalen a la nueva beneficiaria.

4. Validación y registro

Cada proceso de verificación debe ser validado por (***[funciones de las integrantes del equipo encargadas de validar los procesos de verificación en la organización]***).

El hecho de que la beneficiaria haya pasado por el proceso de verificación y haya sido rechazada o aceptada se registra en el historial del caso.