Durante los últimos años, hacer activismo desde organizaciones defensoras de Derechos Humanos y medios de comunicación emergentes se ha convertido en una actividad llena de riesgos cada vez más grandes y complejos. Por otro lado, la naturaleza misma de este tipo de organizaciones dificulta que las prácticas perduren en el tiempo debido a fluctuaciones presupuestarias, y de equipo entre otras, dificultando seriamente la preparación y respuesta ante las crecientes amenazas.

Este manual busca complementar el trabajo que inició la comunidad de facilitadores e implementadores en seguridad dentro de la sociedad civil, poniendo a disposición de estos y de las propias organizaciones beneficiarias un conjunto de actividades que permiten generar políticas de seguridad organizacional cónsonas con las necesidades reales de cada organización, adaptables a los cambios y perdurables en el tiempo.

Seguros y Documentados para el Activismo

SDA

sdamanual.org

# SDA

## Seguros y Documentados para el activismo

sdamanual.org

Edición_ 2018
Edición en ingles_2018
Hecho en Chile

sdamanual.org
Autor_Carlos Guerra Merlo
Diseño y diagramación_ Andrés Alaerkhon-S.
Traducción al Inglés_ Andrés Alaerkhon-S.
Colaboradores_Mario Felaco
_Oriana Hernandez


Manual desarrollado en el marco del Open Web Fellowship de la **Ford Foundation** y **Mozilla Foundation** dentro de la organización **Derechos Digitales América Latina**

# 00_Inicio

# 01_ Licencia

Cuando mencionamos la licencia de este material nos referimos a la licencia con la cual se publica el repositorio de donde se extrae el contenido usado en este material, disponible en https://github.com/cguerrave/SDA para el momento de la publicación. Cuando en la licencia se habla de software aplica al contenido.

MIT License

Copyright (c) 2018 Carlos Guerra

Se concede permiso, de forma gratuita, a cualquier persona que obtenga una copia de este software y los archivos de documentación asociados (el "Software"), para tratar en el Software sin restricciones, incluidos, entre otros, los derechos para usar, copiar, modificar, fusionar, publicar, distribuir, sublicenciar y / o vender copias del software, y para permitir a las personas a quienes se refiere el software equipado para hacerlo, sujeto a las siguientes condiciones:

El aviso de copyright anterior y este aviso de permiso se incluirán en todos copias o porciones sustanciales del software

EL SOFTWARE SE PROPORCIONA "TAL CUAL", SIN GARANTÍA DE NINGÚN TIPO, EXPRESA O IMPLÍCITA, INCLUIDAS, ENTRE OTRAS, LAS GARANTÍAS DE COMERCIALIZACIÓN, APTITUD PARA UN PROPÓSITO PARTICULAR Y NO INFRACCIÓN. EN NINGÚN CASO LOS AUTORES O LOS TITULARES DE LOS DERECHOS DE AUTOR SERÁN RESPONSABLES DE CUALQUIER RECLAMACIÓN, DAÑOS U OTRAS RESPONSABILIDADES, YA SEA EN UNA ACCIÓN CONTRACTUAL, AGRAVIO O DE OTRO TIPO, DERIVADA DE, FUERA DE O EN RELACIÓN CON EL SOFTWARE O EL USO U OTROS TRATOS EN EL SOFTWARE.



Copyright (c) 2018 Carlos Guerra

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

# 02_ Introducción

Desde hace mucho años, las organizaciones defensoras de los Derechos Humanos y medios de comunicación emergentes han enfrentado un sinfín de amenazas realizadas y potenciales, ya sea por parte de estados autoritarios, intereses empresariales, organizaciones extremistas o grupos afectados entre muchos otros. Tomando esto en cuenta, la necesidad de seguridad en las operaciones de este tipo de organizaciones no ha hecho sino crecer, aumentando exponencialmente en la última década cuando se masifica la integración de diferentes soluciones tecnológicas disponibles a las operaciones de las organizaciones. Mientras tanto, desde la industria privada y organismos regulatorios, se comenzaron a desarrollar especificaciones, marcos de referencia y metodologías para generar políticas y protocolos de seguridad que permitieran proteger de forma adecuada los datos y recursos de las empresas y las hicieran cumplir con la ley. Sin embargo, los marcos de referencia desarrollados resultaron sumamente complejos, largos y costosos de implementar para la mayoría de las organizaciones de la sociedad civil que manejan presupuestos ajustados y ciclos de financiamiento inconstantes, lo que condujo en que implementar políticas formales de seguridad fuera privativo y lejano para la mayoría de las organizaciones de la sociedad civil.

Para atacar este problema, surgieron muchas iniciativas que buscaron aumentar el conocimiento en seguridad de la información de las organizaciones de la sociedad civil y activistas, ayudándolos a generar criterios de selección de herramientas y de diseño de procesos implementando medidas de resguardo de la información y otros recursos. Algunas de estas iniciativas fueron más allá y generaron metodologías para evaluar el nivel de seguridad de las organizaciones, adaptar el contenido a grupos específicos u ofrecer herramientas a la comunidad creciente de facilitadores y entrenadores que atienden a las organizaciones que más necesitan implementar seguridad en sus operaciones. Aunque la aparición de estas iniciativas significó una mejora crucial para la seguridad de las organizaciones beneficiarias, siguen quedando algunos espacios en donde se puede optimizar el alcance de las estrategias de seguridad, sobretodo para que estas perduren en el tiempo.

Esta guía busca llenar parte de ese espacio adaptando y simplificando las metodologías disponibles bajo estándares de la industria privada y mezclándolas con otros materiales existentes en el área de seguridad para organizaciones de la sociedad civil y con la experiencia de varios implementadores de seguridad de la información en campo con organizaciones defensoras de Derechos Humanos y medios de comunicación independientes en Latinoamérica durante aproximadamente 5 años para el momento de publicación de esta guía.

Mas específicamente, esta guía excluye deliberadamente ciertos procesos y políticas ampliamente abordadas en materiales dirigidos a la industria privada en función de reducir a lo esencial la cantidad de actividades y tiempo que se debe invertir en su ejecución, entendiendo que las organizaciones objetivo normalmente carecen del tiempo, recursos o personal para desarrollar una estrategia de seguridad tan rigurosa como lo proponen los estándares disponibles como NIST, COBIT o ISO entre otras. En el caso de que una organización desee profundizar en el desarrollo de políticas y estrategias de seguridad más allá de esta guía, en la sección de referencias se ponen a disposición enlaces o contenidos que desarrollan algunos frameworks y metodologías para construir documentación sobre seguridad para organizaciones.

# 03_¿Para quién es esta guía?

En principio, esta guía fue diseñada para ser usada por facilitadores en seguridad de la información que deseen complementar su trabajo de capacitación y/o acompañamiento en organizaciones de la sociedad civil (especialmente organizaciones defensoras de los Derechos Humanos y medios de comunicación independientes). Sin embargo, la misma puede ser aplicada por personas dentro de este tipo de organizaciones, facilitadores externos no relacionados directamente con seguridad de la información que se interesen en el tema y prácticamente cualquier persona interesada que se sienta cómoda en seguir las instrucciones de las actividades.

El contenido de esta guía también puede ser adaptado a cualquier otro tipo de organización que maneje información sensible, desee aumentar la seguridad en el manejo de la misma, y desee documentar políticas de seguridad que perduren en el tiempo.



## Objetivos de la aplicación de esta guía

- Construir políticas y procedimientos de seguridad para organizaciones de la sociedad civil que se adapten a la operación de estas y respondan a las necesidades de sus contextos cambiantes y proyección en el futuro.
- Aumentar el entendimiento del contexto de seguridad en los integrantes de las organizaciones de la sociedad civil en riesgo.
- Introducir a las organizaciones de sociedad civil (especialmente a las organizaciones defensoras de los Derecho Humanos y medios de comunicación independientes) en el modelo de amenazas, y el análisis de riesgo, así como otras metodologías básicas de levantamiento y evaluación del nivel seguridad organizacional.

# 04_ Metodología

## ¿Cómo está estructurada la guía?

Esta guía está dividida en 3 secciones principales, las cuales contienen un grupo de actividades:

En la primera sección se busca explorar el contexto de la organización y algunos de sus procesos internos, una vez levantada la información se establecen las bases de las primeras políticas de seguridad de la organización (Política de clasificación de información y política de retención de datos).

La segunda sección desarrolla una por una otras políticas de seguridad a través de actividades facilitadas, mientras que la tercera sección introduce y orienta en la construcción de los conceptos de modelos de amenazas y procedimientos de seguridad, haciendo énfasis en la creación de matrices de riesgo, planes de sucesión, de comunicaciones y secuencia del protocolo.

Al final se expone una sección de referencias que recopila enlaces de proyectos, bibliografía e iniciativas que complementan las actividades cubiertas, así como los próximos pasos para ampliar, profundizar y perfeccionar las políticas construidas con este material.



En cada sección se propone un conjunto de actividades que explican el proceso de facilitación que se debe seguir para generar los productos propuestos, cada actividad tiene la siguiente información:

- Tiempo estimado de realización de la actividad, el cual puede variar en función del tamaño del grupo, la destreza del facilitador y los pasos considerados en cada actividad para ejecutar.
- Preparación previa de la actividad en términos de investigación o levantamiento de datos de la organización.
- Materiales requeridos para ejecutar la actividad.
- Instrucciones de la actividad, normalmente en una secuencia de pasos con las acciones a realizar y en los casos que aplique gráficos descriptivos.
- Cierre de la actividad en donde se hace un recuento de lo que se logró y para qué servirán los productos generados.
- Referencias que se hacen durante el desarrollo de la actividad.

## Sobre las referencias en este manual

Las referencias están numeradas en la versión impresa y pueden ser consultadas desde un explorador web de la siguiente manera:

Ingresando a:

- sdamanual.org/es/referencias, navegar a la referencia de interés y hacer clic

# 01_ Exploración y Objetivos de Seguridad

## _ Conceptos

- Actores:
Personas, grupos u organizaciones formales o informales que interactúan con nuestra organización dentro de un espectro que va desde aliados hasta adversarios.

- Medios de transmisión de información:
Canales usados para transferir información entre el equipo de trabajo o entre la organización y actores externos. Aplica tanto para canales físicos tradicionales como para medios digitales.

- Lugares de reposo de la información:
Lugares físicos y digitales en donde la información se almacena para ser usada, transmitida o archivada. En el ámbito digital coincide mayormente con dispositivos.

- Nivel de impacto:
gravedad de las consecuencias negativas que pueden experimentarse luego de concretarse un hecho específico.



# 01_ Objetivos de la organización

Tiempo estimado: 20 min

## _Justificación

Esta actividad busca poner a todo el grupo en la misma página en cuanto a las razones de ser de la organización y las metas que persigue. En el caso de las organizaciones de activismo, este puede ser un momento propicio para afianzar los conceptos y valores de justicia social que motivan al grupo para hacer el trabajo que hacen. En el caso de los medios de comunicación se pueden afianzar los valores de acceso a la información veraz y libertad de expresión que motivan a los periodistas a ejercer su labor.

Este apartado busca que los participantes dejen a un lado el estrés producido por las altas cargas de trabajo para concentrarse en las motivaciones internas que llevan a cada uno a ser parte del equipo, sirviendo además como rompe hielo para afrontar mejor el desarrollo de las siguientes actividades.

## _Datos de entrada

_Misión, Visión, y Objetivos de la organización.

## _Productos

### _Directos

- Mapa de motivos por los cuales la organización existe desde el punto de vista de los participantes.

### _Indirectos

- Conciencia colectiva en función a los objetivos de la organización.
- Similitudes o discrepancias entre la percepción del equipo y la función formal de la organización.

## _Preparación previa

Revisar si existe de forma pública, misión, visión, y objetivos de la organización y preparar el material correspondiente.

## _Materiales

- Notas adhesivas para los participantes.
- Papeles impresos o escritos con la misión, visión, y objetivos formales escritos de la organización o sus equivalentes en caso de que estén planteados de forma distinta.

## _ Instrucciones

Dependiendo de la cantidad de participantes y de la comodidad del facilitador, se requiere la realización de los siguientes pasos ya sea en forma individual o en parejas

**1.** Distribuir entre los participantes una cantidad adecuada de notas adhesivas y marcadores.

**2.** Pedir a los participantes que se tomen 5 minutos para escribir en las notas adhesivas las razones por las cuales la organización existe, puede ser de ayuda plantear oraciones para completar como:

- La organización existe para..
- Una razón de ser de la organización es...

**3.** Luego de 5 minutos, pedir a los participantes que peguen las notas adhesivas en un lugar definido, y se tomen unos minutos adicionales para agrupar las notas que estén repetidas o sean muy afines. Es importante que quede en evidencia fácilmente cuando un mismo grupo tenga varias notas asociadas, por lo que no se recomienda tapar por completo las notas similares.

**4.** Realizar un recuento de lo que se recopiló haciendo especial énfasis en las ideas comunes.

**5.** Mostrar la misión, visión, y objetivos formales disponibles discutiendo brevemente sobre las similitudes y/o discrepancias que puedan existir entre lo recopilado en la lluvia de ideas, y lo que está formalmente escrito. En caso de encontrar diferencias muy marcadas, podría ser una señal de que:

- La organización debe actualizar sus documentos formales para reflejar su evolución y estado actual.
- La organización se desvió de sus intenciones iniciales, y debería plantear reconducir sus acciones para insertarse con éxito en lo propuesto inicialmente.

En cualquier caso, no es responsabilidad del facilitador iniciar una discusión a fondo sobre estas diferencias, sino invitar a la reflexión y a la revisión en un momento adecuado para la organización, manteniendo un lenguaje amigable y respetuoso al reconocer el valor que tuvo el ejercicio. Para esta metodología saber cómo funciona la organización **hoy** es suficiente para continuar con las actividades, por lo que dichas discrepancias no deberían afectar el éxito de la sesión de trabajo.

## _Referencias


**R1** A Step-by-Step Exercise for Creating a Mission Statement




# 02_ Mapeo y Clasificación de actores

Tiempo estimado: 20 min

Esta actividad está basada en la sección Expanding our knowledge of actors de la guía de Seguridad Holística de Tachtical Technology Collective disponible en las referencias.

## _Justificación

En esta actividad la idea es seguir explorando la organización, recopilando información directamente relacionada con la seguridad de la misma, la cual es necesaria para levantar un modelo de amenazas óptimo en lo sucesivo. Además, resulta un insumo valioso para estudiar la evolución de la organización, su entorno, y los cambios en el modelo de amenazas correspondiente.

## _Datos de entrada

- Personas, grupos e instituciones relacionadas a la organización.
- Proyectos y procesos medulares de la organización.
- Información que maneja la organización en sus procesos.
- Posibles consecuencias negativas al vulnerar la información que maneja la organización.

## _Productos

### Directos

- Mapa de actores.

### Indirectos

- Conciencia grupal sobre los actores relacionados a la organización.

## _Preparación previa

Haber investigado lo suficiente a la organización como para tener ideas claras de sus actores asociados. Esto con la idea de iniciar o reanudar la lluvia de ideas en el caso de que el grupo se sienta estancado o lento durante la actividad.

## _Materiales

En caso de realizar la actividad en físico:

- Notas adhesivas y marcadores o
- Piezas grandes de papel para pegar en la pared y marcadores.

En caso de realizar la actividad en digital:

- Computadora
- Proyector
- Hoja de cálculo lista para llenar, mostrando los encabezados con categorías de actores asociados.

## _ Instrucciones

Una vez relacionados los objetivos de la organización en la actividad anterior, debería ser más claro para los participantes el enfoque que tiene el grupo, y qué tipo de actores están vinculados a su trabajo, además de las motivaciones de dichos actores de cara a la seguridad de la organización.

**1.** Explicar brevemente que la idea es crear un espectro de aliados ordenados por su actitud ante la organización, buscando emplear pocas opciones para facilitar el proceso. Por ejemplo:

- Oponentes activos
- Oponentes
- Actores neutrales
- Aliados
- Aliados activos

Si el grupo y el facilitador lo consideran necesario, podrán dedicar unos minutos a discutir acerca de los criterios por los cuales se desarrollarían las categorías a estudiar.

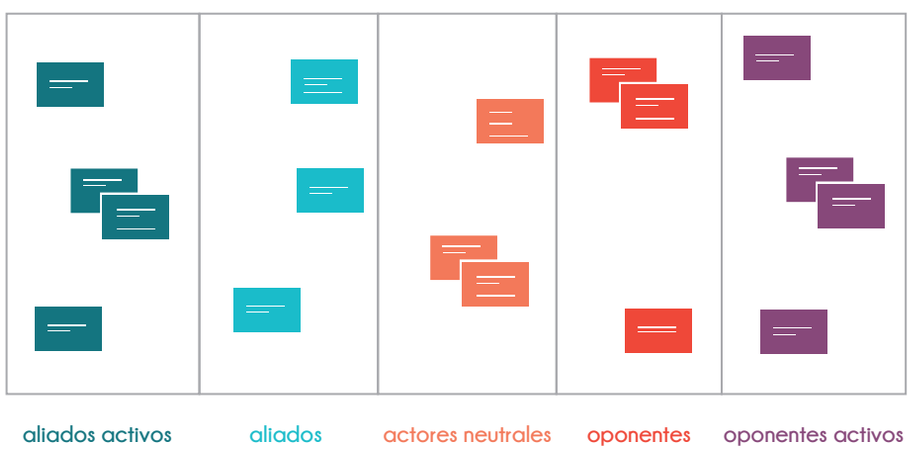



Grafico 1. Mapeo de actores de una organización.



**2.** Explicar brevemente que se consideran actores a: personas, grupos e instituciones sin importar su formalidad en tanto cuenten con alguna relación existente o potencial con la organización. Por ejemplo es buen hábito no olvidar actores como:

- Entes reguladores (impuestos, trabajo, comunicaciones).
- Empresas de servicios públicos.
- Proveedores.
- Personal de mantenimiento y servicios generales.
- Personas a las que se prestan servicios (víctimas, grupos desprotegidos, ciudadanos buscando asesoría, etc.).
- Organizaciones similares.

**3.** Pedir a los participantes que digan y/o escriban los actores, para luego ser colocados en las columnas en donde consideren que van ubicados según su juicio. Si hay alguna discrepancia con el resto del público en la categoría elegida se puede discutir al respecto hasta que haya consenso y el grupo esté conforme con todos los actores en la lista.

**4.** Una vez que la lista se considere completa preguntar a los participantes por aquellos actores que se encuentran en los extremos (oponentes y aliados activos en el ejemplo anterior). La idea es discutir sobre las capacidades y las motivaciones de estos actores para perjudicar o ayudar a la organización y preparar a los participantes para las actividades de mapeo de datos y modelo de amenazas.

**5.** Discutir con los participantes sobre algunas consideraciones del mapeo de actores:

- Los mapas de actores pueden variar en el tiempo de forma muy rápida. Hoy un aliado activo mañana puede ser un oponente activo, o un actor neutral puede tomar partido a raíz de un evento particular.
- La categorización de los actores es perceptual, quizás para un grupo cierto actor parece un aliado, pero en la práctica puede jugar un papel diferente desconocido para la organización.
- Generalmente una organización está vinculada a muchos más actores de los que se pueden obtener en una lluvia de ideas de 10 minutos. Vale la pena que el grupo se sienta cómodo con la metodología para que puedan replicarla por su cuenta cuando lo consideren conveniente.

Es importante que el mapa obtenido se encuentre disponible para futuras actividades, si se hace en físico se recomienda no desmontar los papeles y/o notas adhesivas, sino moverlos a un lugar en donde sean visibles y no interfieran con las demás actividades. En caso de hacer la actividad en digital, se recomienda tener a la mano el archivo en donde se recopiló la información.

## _Referencias

R2 Holistic Security: 2.3 Vision, Strategy and Actors Security First: ChampionsCurriculum

# 03_ Mapeo y Clasificación de Información

Tiempo estimado: 90 min

Esta actividad es una variación propuesta de una dinámica planteada en varios recursos como Holistic Security en su sección "2.4 Understanding and Cataloguing our Information" de de Tactical Technology Collective o SaferJourno de Internews entre otros.

La idea de esta actividad es mapear todos los objetos de datos que maneja la organización, pensar en las posibles consecuencias que tendría el compromiso de estos objetos, esquematizar estas posibles consecuencias en una matriz de impactos, y asociar los objetos de información manejados con los niveles de impacto en la matriz construida.

## _Justificación

La idea de esta actividad es completar la recopilación de información sobre la organización, y así redirigir la misma hacia la sensibilidad de la información. En el proceso se establecerán las bases que permitirán construir las primeras políticas de seguridad para la organización.

## _Datos de entrada

- Mapa de actores.

## _Productos

### Directos

- Matriz de consecuencias posibles.
- Mapa de datos con impacto por vulneraciones asociadas.

### Indirectos

- Conciencia grupal sobre los actores relacionados a la organización.
- Criterios de clasificación de información dentro de la organización.

## _Preparación previa

En caso de realizar la actividad en digital, se sugiere disponer de una hoja de cálculo u otro software con todos los campos y formatos necesarios.

## _Materiales

En caso de realizar la actividad en físico:

- Notas adhesivas y marcadores o
- Piezas grandes de papel para pegar en la pared y marcadores.



En caso de realizar la actividad en digital:

- Computadora
- Proyector
- Hoja de cálculo lista para llenar, mostrando los encabezados con categorías de actores asociados.

## _Instrucciones

**1.** Realizar una lluvia de ideas con las piezas de información que maneja la organización, estas pueden incluir desde denuncias de víctimas, documentos filtrados, investigaciones en construcción hasta libros contables, publicaciones en redes sociales y/o informes públicos. Ninguna pieza de información legítima es poco relevante para este ejercicio.

- Es especialmente relevante considerar información en físico.
- Cada idea se debe colocar en una nota adhesiva o equivalente y estar a la vista de todos.
- Se puede avanzar cuando exista consenso entre los participantes.
- Se pueden agregar más ítems durante el resto de la actividad.


Grafico 2. Mapeo de piezas de información

**2.** Con las piezas de información a la vista, explicar brevemente los conceptos de Disponibilidad, Integridad y Confidencialidad, los cuales son utilizados frecuentemente en seguridad de la información para explicar los diferentes tipos de compromiso de la información. Se sugiere desarrollar conceptos breves y revisar otras referencias para tener un entendimiento más amplio:

**Disponibilidad:** Es la capacidad de estar siempre al alcance de quien la necesite. Por ejemplo, cuando un servidor se queda sin electricidad atenta contra la disponibilidad de la información contenida en el mismo.

**Integridad:** Es la capacidad de ser confiable, en el mero sentido de que su contenido no ha sido manipulado o alterado por un tercero. Por ejemplo, que un tercero malintencionado tome una base de datos de víctimas y modifique la información se considera una amenaza a la integridad de esa base de datos.

**Confidencialidad:** Es la capacidad de ser accesible sólo a quienes corresponde por definición. Por ejemplo, cuando un tercero puede leer correos electrónicos que se envían dos personas se considera una amenaza a la confidencialidad de la información transmitida por el correo.

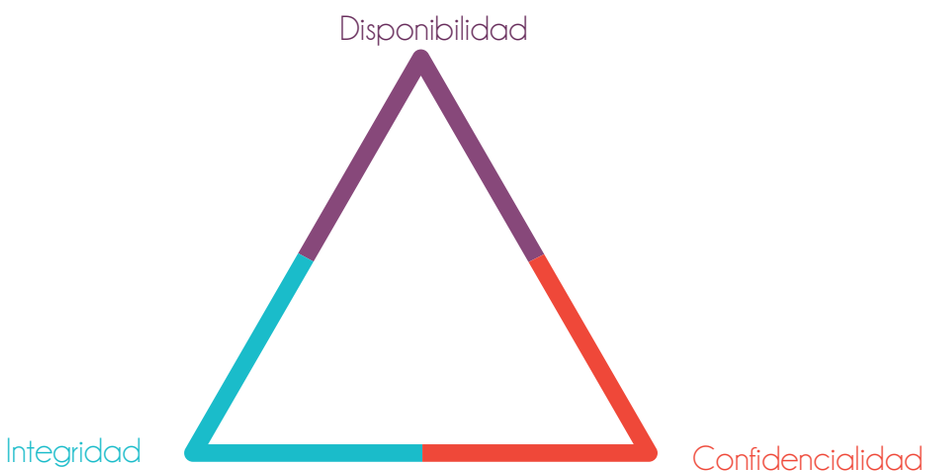



Grafico 3. Triada CIA (Confidenfiality-Integrity-Availability).



**3.** Conversar con los participantes sobre los tipos de consecuencias negativas que puede afrontar la organización ante algún compromiso de la información que se maneja. Crear aparte de la lluvia de ideas de piezas de información una lista horizontal con los tipos de con secuencias como se muestra en la figura 4.

| Consecuencias Digitales | Consecuencias Físicas | Consecuencias Emocionales | Consecuencias Judiciales | Consecuencias Administrativas | Consecuencias Económicas |
|---|---|---|---|---|---|
| | | | | | |

Grafico 4. Tipos de Consecuencias

**3.** La idea es generar una matriz cuyo eje horizontal corresponda a esta clasificación de consecuencias, una propuesta completa (o simplificada dependiendo del facilitador y del grupo) puede ser la que se encuentra a continuación:

- Consecuencias digitales: Que afecten la presencia online o recursos digitales de la organización. Por ejemplo, relacionadas a los medios sociales, servidores, cuentas de correo, servicios usados por el equipo interno, etc.
- Consecuencias físicas: Son las relacionadas a la integridad de personas, objetos y espacios. Por ejemplo, agresiones físicas, muerte, destrucción de espacios, pérdida de recursos, etc.
- Consecuencias emocionales: Son las relacionadas al bienestar psicosocial de las personas involucradas con la organización, esto no solo incluye al equipo sino también a proveedores, beneficiarios, víctimas, etc. Normalmente están relacionados a situaciones que crean miedos, estrés, fatiga y traumas a los actores relacionados.
- Consecuencias judiciales: Son aquellas que afectan la integridad judicial de personas asociadas a la organización. Por lo general, están relacionadas a arrestos, retenciones, allanamientos, juicios, etc.
- Consecuencias administrativas: Son aquellas relacionadas al estado legal de organizaciones y personas más allá de lo judicial. Frecuentemente relacionadas al cumplimiento de regulaciones, impuestos, inspecciones, pérdida de la figura legal de la organización, infracciones a leyes, etc.
- Consecuencias económicas: Son aquellas relacionadas directamente a la pérdida de dinero y bienes por parte de la organización y/o sus integrantes.

Estos tipos de consecuencias son propuestos, en el caso de querer simplificar el ejercicio se pueden combinar o excluir explícitamente algunos de los ejes propuestos, incluso si el equipo lo considera pertinente se pueden agregar nuevos tipos. Por ejemplo, consecuencias de imagen o religiosas (si aplican).



**4.** Teniendo claro los tipos de consecuencias, se sugiere pedir a los participantes que piensen en posibles consecuencias producto del compromiso de las piezas de información mapeadas en términos de disponibilidad, integridad y confidencialidad, tomar notas de estos y colocarlos en notas adhesivas o su equivalente digital debajo del tipo de consecuencia al que pertenece (digital, físico, legal, etc.)

- Es normal y esperado que muchas consecuencias se repitan, en estos casos con la nota adhesiva o equivalente ya existente será suficiente.
- Pensar en disponibilidad, integridad y confidencialidad es una ayuda para facilitar la discusión y la lluvia de ideas de consecuencias, sin embargo, si el equipo se siente cómodo planteando las consecuencias posibles en otros términos puede funcionar sin problemas siempre y cuando representen consecuencias posibles y puedan ser priorizadas en el siguiente paso.
- Es normal que el compromiso de una pieza de información pueda tener consecuencias en más de un eje.

Algunos ejemplos de consecuencias pueden ser:

- Pérdida de la figura jurídica de la organización (Consecuencia administrativa).
- Muerte de denunciantes (Consecuencia física).
- Agresiones a beneficiarios (Consecuencia física).
- Multa excesiva (consecuencia económica).
- Renuncia o despido de personal (Consecuencia administrativa).
- Pérdida del sitio web (Consecuencia digital).
- Allanamiento de la sede (Consciencia judicial).
- Aumento drástico de niveles de estrés en el equipo de trabajo (consecuencia emocional).
- Aumento excesivo de la carga de trabajo del equipo (consecuencia emocional).

| ▪ Consecuencias Digitales | ▪ Consecuencias Físicas | ▪ Consecuencias Emocionales | ▪ Consecuencias Juridicas | ▪ Consecuencias Administrativas | ▪ Consecuencias Económicas |
|---|---|---|---|---|---|
| La organización se queda sin Sitio Web | Muerte de Beneficiario o Equipo | Carga de Trabajo / estres inmanejable | Arresto | Pérdida de Figura Juridica | Pérdidas Pequeñas de dinero/equipos |
| La organización se queda sin Cuenta Twitter | Agresiones físicas a personas | Evento traumático a personas | Allanamiento | Multas excesivas | Quiebra de la Organización |
| La organización se queda sin Correos Electrónicos | Destrucción de oficina | | Juicio | Monitoreo Administrativo excesivo | Pérdidas Importantes de dinero/equipos |
| La oficina se queda sin internet | Destrucción de Equipos | | Prohibición de Salida del país de miembro | | |
| Se filtran los datos de los denunciantes | | | | | |
| Se filtran los libros contables | | | | | |

Grafico 5. Mapeo de Consecuencias.

**5.** Luego de obtener algunas consecuencias de cada uno de los tipos definidos se introduce la idea de calificar las consecuencias mapeadas según su nivel de impacto, se propone crear un eje vertical que represente impactos nulos, bajos, medios y altos. En el caso de que el facilitador y el equipo se sientan cómodos al respecto, se puede cambiar esta escala a cualquier otra que se considere conveniente (del 1 al 10, agregar a la propuesta impacto crítico, etc.). Luego de creado este eje se procede a ubicar con el apoyo del equipo las amenazas mapeadas en las distintas categorías como se muestra en la figura. Algunas consideraciones son:

- Es posible que algunos espacios queden en blanco, dependiendo del caso vale la pena preguntarle al equipo qué consecuencias están faltando en esos espacios. En el caso de impactos bajos o nulos no es obligatorio colocar consecuencias directas, esto se puede explicar con que todo lo que se considere por debajo de la consecuencia con menor impacto es irrelevante en términos de riesgos.

- A esta parte de la actividad se le debe dedicar un tiempo adecuado ya que representa el pilar de la primera política de seguridad de la organización (clasificación de información).

| | ▪ Consecuencias Digitales | ▪ Consecuencias Físicas | ▪ Consecuencias Emocionales | ▪ Consecuencias Juridicas | ▪ Consecuencias Administrativas | ▪ Consecuencias Económicas |
|---|---|---|---|---|---|---|
| ALTO | Se filtran los datos de los denunciantes | Muerte de Beneficiario o Equipo | Evento traumáticoa personas | Arresto | Pérdida de Figura Juridica | Quiebra de la Organización |
| | La organización se queda sin Correos Electrónicos | Agresiones físicas a personas | | | | |
| MEDIO | La organización se queda sin Cuenta Twitter | Destrucción de oficina | Carga de Trabajo / estres inmanejable | Allanamiento | Multas | Pérdidas Importantes de dinero/equipos |
| | La organización se queda sin Sitio Web | | | Juicio | | |
| | | | | Prohibición de Salida del país de miembro | | |
| BAJO | La oficina se queda sin internet | Destrucción de Equipos | | | Monitoreo Administrativo excesivo | Pérdidas Pequeñas de dinero/equipos |
| NULO | Se filtran los libros contables | | | | | |

Grafico 6. Niveles de Impacto.

6. Una vez que el equipo esté conforme con la matriz de consecuencias, se pueden asociar los objetos de datos mapeados al comienzo de la actividad con el nivel de impacto de las consecuencias correspondientes al compromiso. Esto puede hacerse de múltiples formas, una propuesta se dispone en el siguiente grafico.

## _Cierre de la actividad

Al finalizar la actividad se puede discutir y hacer énfasis en lo que se logró:

- Se definieron ejes de consecuencias y se asociaron a la información que la organización maneja.
- Se establecieron las bases de la política de clasificación de información, así cada vez que se maneje un nuevo objeto o pieza de información se puede determinar el nivel de impacto asociado al compromiso de este, y con los productos que se generarán más adelante se puede determinar con facilidad qué medidas de seguridad se deben tomar al manipular estos nuevos objetos de datos.

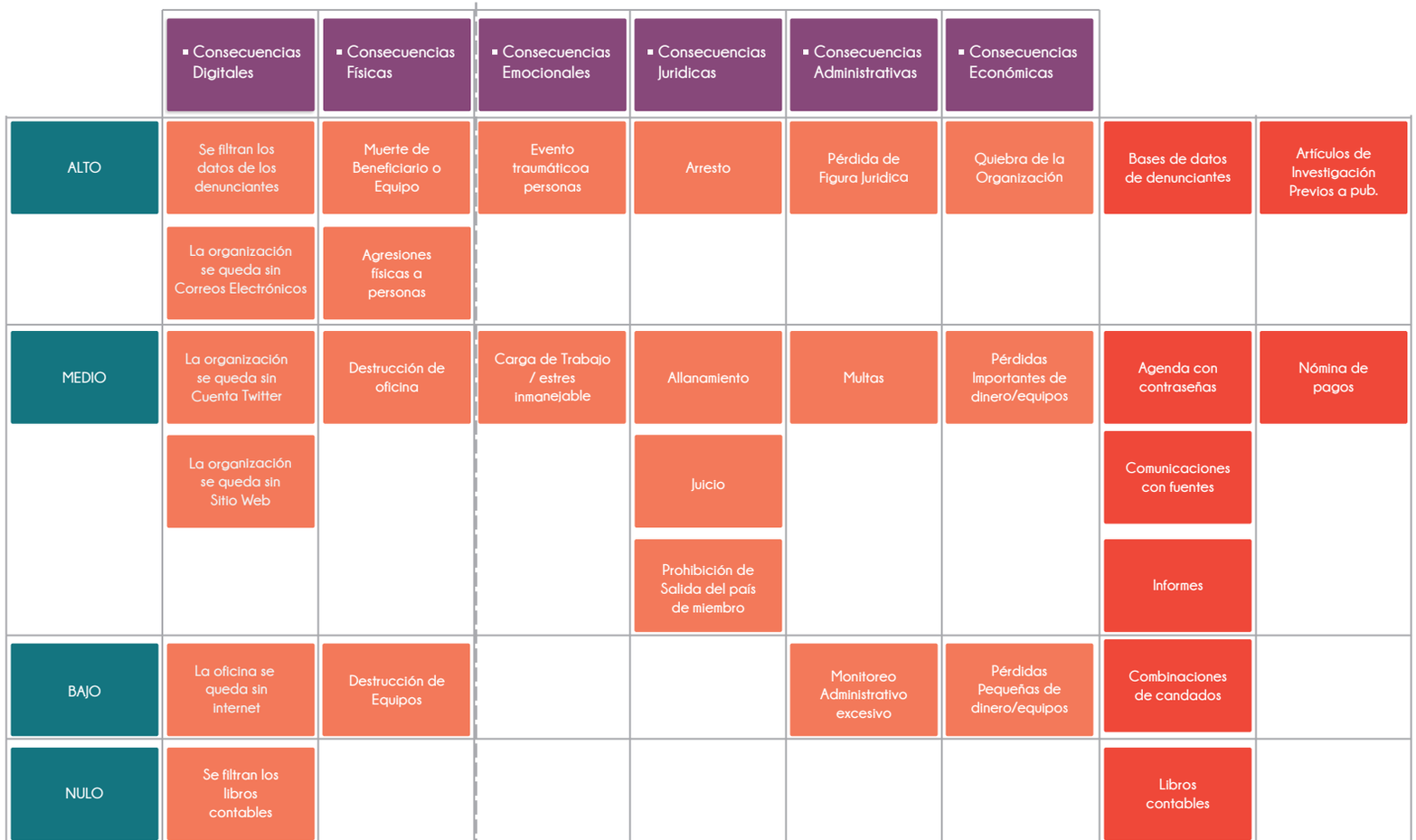



Grafico 7. Objetos de datos ordenados por nivel de impacto.

## _Referencias


R3 Holistic Security: 2.4 Understanding and Cataloguing our Information
R4 SaferJourno
R5 Security First: ChampionsCurriculum
R6 Wikipedia: Seguridad de la información

# 04_ Mapeo de flujo de Información

Tiempo estimado: 90 min

## _Justificación

La idea en esta actividad es entender en dónde reposa la información, a través de cuales canales se transmite la información, discutir los niveles de seguridad que brindan estos canales, y asociar los objetos de datos mapeados en la actividad anterior para definir factores clave en la construcción de una política de retención de datos.

## _Datos de entrada

- Matriz de consecuencias posibles.
- Mapa de datos con impacto por vulneraciones asociadas.

## _Productos

### Directos

- Mapa de datos según los lugares en dónde reposan.
- Mapa de datos según los canales por donde se transmiten.
- Análisis básico de seguridad de lugares de reposo y canales de transmisión de datos.
- Directivas básicas sobre el manejo de información según su nivel de sensibilidad.

### Indirectos

- Criterios de selección de canales de transmisión y lugares de reposo seguros para la información.
- Conocimiento de qué canales de transmisión y cuales lugares de reposo se deben emplear con objetos de datos existentes y nuevos.

## _Preparación previa

En caso de realizar la actividad en digital, se sugiere disponer de una hoja de cálculo u otro software con todos los campos y formatos necesarios.

## _Materiales

En caso de realizar la actividad en físico:

- Notas adhesivas y marcadores o un equivalente digital al igual que en las actividades anteriores.
- Hojas de papel grandes.

En caso de realizar la actividad en digital:

- Computadora
- Proyector
- Hoja de cálculo lista para llenar, mostrando los encabezados con categorías.

## _Instrucciones

**1.** Pedir a los participantes que piensen y compartan los lugares y dispositivos en donde reposa la información de la organización. Estos pueden ser físicos y digitales, con estos lugares se puede construir encabezados de columnas como se muestra en la figura 8 :

Algunos ejemplos que pueden ayudar al grupo a desarrollar mejor la lluvia de ideas son:

- Computadoras portátiles y de escritorio.
- Unidades USB.
- Archivadores.
- Discos duros externos.
- Escritorios.
- CD's.
- Servidor interno.
- Servicios de almacenaje en la nube como Dropbox o Google Drive.
- Teléfonos móviles.
- Software administrativo y/o contable.

| | | | | |
|---|---|---|---|---|
| ◆ Escritorios | ◆ Computadoras portátiles | ◆ Teléfonos celulares | ◆ Memorias USB | ◆ Dropbox |
| | | | | |

Grafico 8. Lugares de almacenamiento de información

2. Continuar la lluvia de ideas pero ahora preguntando a los participantes a través de cuales medios se transmite la información. Agregar las respuestas a la lista anterior como muestra el gráfico:

Algunos ejemplos que pueden ayudar al grupo a desarrollar mejor la lluvia de ideas son:

- Correo electrónico convencional.
- Servicios de mensajería (Whatsapp, Signal o Telegram).
- Correo físico.
- Llamadas telefónicas.
- Mensajes de texto SMS.
- Servicios de correo cifrado como Protonmail, Hushmail o Tutanota.
- Redes sociales.
- Sitio Web.
- Administración remota de equipos

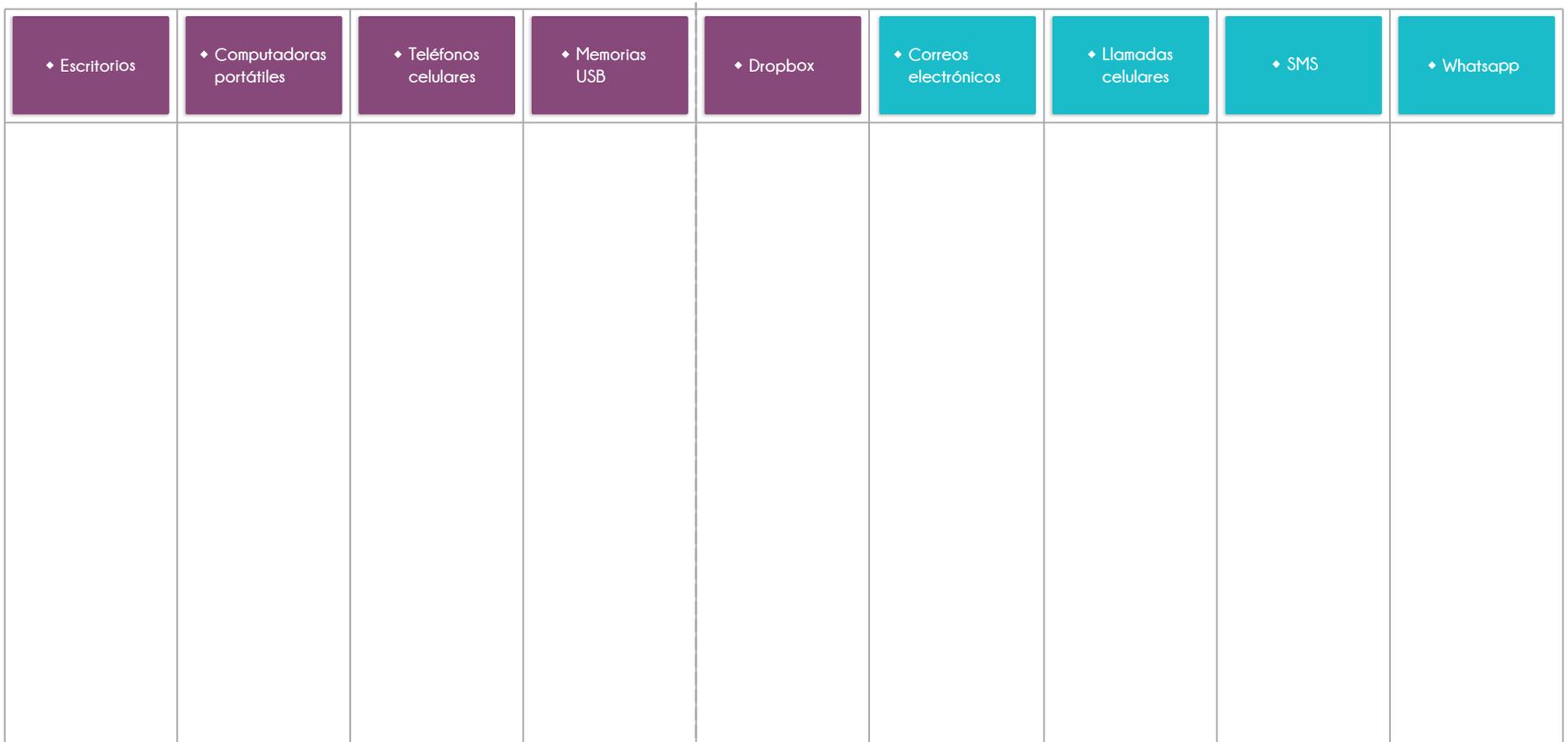



Grafico 9. Canales de transmisión de la información

3. Pensando en los encabezados de las columnas escritos como uno de los ejes de una matriz, colocar en el eje vertical los niveles de impacto usados en la actividad anterior:

- Debemos tener cuidado de utilizar los mismos niveles de impacto en caso de que hayan sido definidos de diferente forma a los propuestos en esta guía.

| | ◆ Escritorios | ◆ Computadoras portátiles | ◆ Teléfonos celulares | ◆ Memorias USB | ◆ Dropbox | ◆ Correos electrónicos | ◆ Llamadas celulares | ◆ SMS | ◆ Whatsapp |
|---|---|---|---|---|---|---|---|---|---|
| ALTO | | | | | | | | | |
| MEDIO | | | | | | | | | |
| BAJO | | | | | | | | | |
| NULO | | | | | | | | | |

Grafico 10 Niveles de impacto.

**4.** Preguntar por los objetos de datos en cada nivel de impacto en donde se almacenan o se transmiten. Se recomienda no tomar nota de cada objeto de datos, sino marcar cada coincidencia de nivel de impacto asociado con el lugar de almacenaje o medio de transmisión de información. idealmente se recomienda tener la matriz en una hoja grande papel que permita marcar con X en los lugares que corresponda como se muestra en el gráfico 11.

- Este paso puede ser largo, hay que tomar previsiones en la planificación de la agenda.
- Puede ayudar tener las notas adhesivas o equivalentes de la actividad anterior para los objetos de datos por nivel de impacto como guía visual para los participantes.

**5.** Introducir los conceptos que sean pertinentes sobre seguridad para lugares de almacenamiento y canales de transmisión según los ítems que se tengan como lugares de almacenaje y medios de transmisión de información.

- Cifrado., Cifrado punto a punto.
- Seguros, candados, cajas fuertes, etc.
- Accesibilidad de recursos (Quién tiene acceso a qué).
- Consideraciones de servicios en la nube.

El éxito de este paso está muy relacionado con el conocimiento que tenga el facilitador y el grupo sobre los equipos y servicios utilizados. Puede suceder que en alguna actividad aparezcan servicios que el facilitador desconoce, es importante tener la capacidad de preguntar al grupo lo que sepan y de investigar por cuenta propia cualquier consideración de seguridad pertinente al ítem desconocido.

| | | | • Escritorios | • Computadoras portátiles | • Teléfonos celulares | • Memorias USB | • Dropbox | • Correos electrónicos | • Llamadas celulares | • SMS | • Whatsapp |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Bases de datos de denunciantes | Artículos de Investigación Previos a pub. | ALTO | X | X | X | X | | X | X | | X |
| Agenda con contraseñas<br>Comunicaciones con fuentes<br>Informes | Nómina de pagos | MEDIO | X | X | X | X | X | X | X | X | X |
| Combinaciones de candados | | BAJO | | | | | X | | | | |
| Libros contables | | NULO | X | X | | X | | | | | |

Grafico 11. Medios de almacenaje y transmisión de datos por nivel de impacto actualmente empleados por la organización.

**6.** Discutir con el grupo si hay canales que se consideren inseguros donde información sensible se almacene o transmita. Algunas preguntas clave pueden ser:

- ¿Algunos de los anteriores se consideran canales inseguros?.
- ¿Algunos de estos lugares de almacenaje es de fácil acceso para personas no autorizadas?.

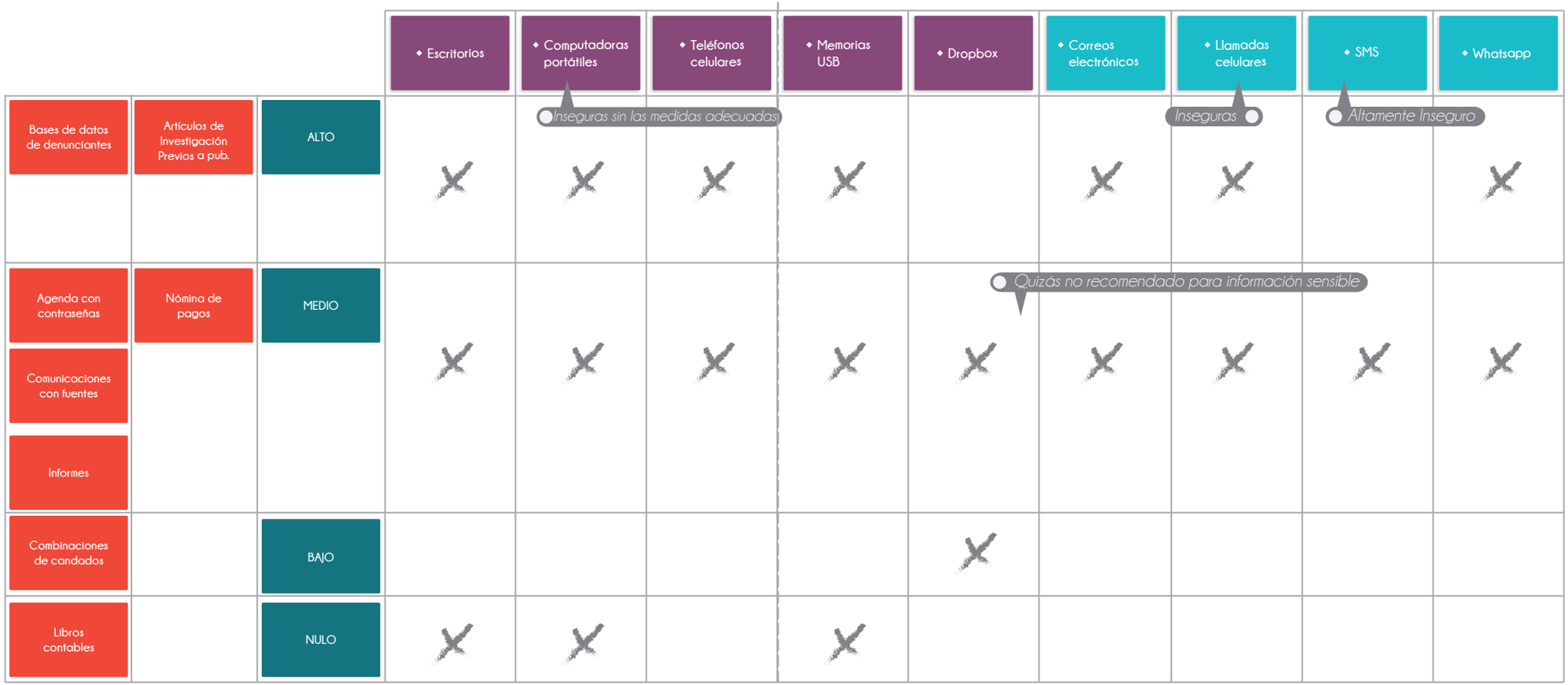





Grafico 12. Discusión de mapa de datos

**7.** Plantear al grupo una modificación en la matriz en donde se defina qué tipo de información por nivel de impacto debe estar en cada columna de la matriz, y las consideraciones pertinentes en cada caso (si un equipo debe estar cifrado para contener cierta información, si se debe usar VPN o https para acceder a un recurso específico, etc.).

- El uso de otro color puede ser beneficioso para trabajar sobre la misma matriz, facilita la actividad para ver mejor las diferencias entre lo que se hace actualmente en la organización y lo que se debería hacer desde ese momento en adelante.

| | | | ◆ Escritorios | ◆ Computadoras portátiles | ◆ Teléfonos celulares | ◆ Memorias USB | ◆ Dropbox | ◆ Correos electrónicos | ◆ Llamadas celulares | ◆ SMS | ◆ Whatsapp |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Bases de datos de denunciantes | Artículos de Investigación Previos a pub. | ALTO | ✗ | ✗ Cifrado de Archivo o Disco | ✗ | ✗ | | ✗ Cifrado con PGP | ✗ | | ✗ SIGNAL |
| Agenda con contraseñas<br>Comunicaciones con fuentes<br>Informes | Nómina de pagos | MEDIO | ✗ Con Política de Escritorio Limpio | ✗ Con Cifrado de Archivo | ✗ Cifrado de Equipo y Clave de Acceso | ✗ | ✗ | ✗ Gmail con Autenticación en 2 Pasos | ✗ | ✗ | ✗ ✗ |
| Combinaciones de candados | | BAJO | ✗ | ✗ | ✗ | | ✗ ✗ | ✗ | ✗ | | ✗ |
| Libros contables | | NULO | ✗ ✗ | ✗ ✗ | ✗ | ✗ ✗ | ✗ | ✗ | ✗ | ✗ Casos de Emergencia | ✗ |

Grafico 13. Medios de almacenaje y transmisión de datos por nivel de impacto propuesto para la organización

## _Cierre de la actividad

Al finalizar la actividad se puede discutir y hacer énfasis en lo que se logró:

- Se mapearon todas las formas de comunicación y los lugares de reposo de la información.
- Se asociaron los objetos de datos de la organización en estos canales y lugares de reposo.
- Se inició la discusión sobre el nivel de seguridad de los medios usados para guardar y transmitir información y se establecieron algunas premisas básicas desde donde se construirá la política de retención de datos de la organización.

Es necesario tomar en cuenta que para elaborar una política de retención de datos completa es importante considerar otras cosas además de los medios de almacenamiento y comunicación de los objetos de datos, por ejemplo:

- Por cuánto tiempo cada objeto de datos debe ser guardado (caducidad de la información).
- De qué forma se deben borrar los objetos de datos por caducidad. Ejemplo: procesar estadísticas anuales de denuncias que se van a borrar.
- Quiénes manejan la información: implementación del principio del mínimo privilegio.
- Quiénes son responsables de la generación, almacenamiento y custodia de la información.



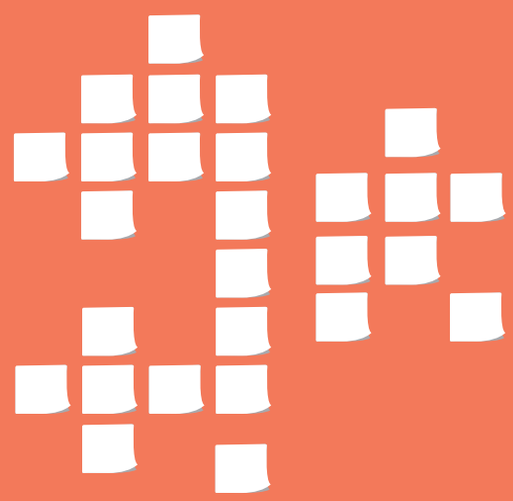
## _Referencias


**R7** ¿Qué es el cifrado? - Surveillance Self Defense | EFF

**R8** Proteger los archivos sensibles en tu computadora - Cifrado de archivos | Security in a box

**R9** Comunicándote con otros - Cifrado punto a punto - Surveillance Self Defense | EFF

**R10** Secure Messaging Scorecard - Evaluación de servicios de mensajería instantánea | EFF - Aunque se encuentra desactualizada sigue siendo un recurso valioso de consultar.



# 02_ Políticas y Directivas

## _ Conceptos

- Política de seguridad:

Documento formal que recopila las estrategias de seguridad que una organización toma en ámbitos específicos de sus operaciones, brindan un panorama general del estado de la seguridad de la organización, los objetivos que persigue en términos de seguridad y criterios para determinar posibles excepciones a la política o acciones a tomar ante situaciones que escapen del alcance actual del documento.

- Directiva de seguridad:

Conjunto de reglas específicas que son implementadas por el equipo de trabajo y sus aliados relevantes para implementar las políticas de seguridad en el trabajo diario. Estas directivas pueden ser más concretas en el uso de herramientas y equipos específicos y pueden cambiar en el tiempo con más frecuencia.



# 01_ Introducción a las políticas y directivas de seguridad

Tiempo estimado: 15 min

## _Justificación

Antes de empezar las actividades que buscan generar documentos conteniendo políticas y directivas de seguridad, es muy importante que los participantes entiendan qué son y para qué sirven, disminuyendo los errores, mejorando el flujo de las actividades e involucrando de mejor manera a los participantes. La idea de esta actividad es introducir los conceptos de políticas y directivas de seguridad.

A diferencia de otras actividades en este manual, la presente es de carácter expositivo y menos interactivo. En la medida en que el facilitador se sienta cómodo puede diseñar una actividad que logre introducir los conceptos.

## _Productos

_Indirectos

Conocimiento del equipo de los conceptos de políticas y directivas de seguridad.

## _Preparación previa

En el caso de requerirlo, algún material audiovisual como presentaciones, videos o papeles con los conceptos abordados y/o ejemplos.

## _Instrucciones

1. Presentar el concepto de política de seguridad al grupo:

> Política de seguridad: Es un documento formal que recopila las estrategias de seguridad que una organización toma en ámbitos específicos de sus operaciones, brindan un panorama general del estado de seguridad de la organización, los objetivos que persigue en términos de seguridad y criterios para determinar posibles excepciones a la política o acciones a tomar ante situaciones que escapen al alcance actual del documento.

Este concepto puede ser planteado como la unión de varias ideas:

- Es un documento escrito.
- Describe objetivos y estrategias de seguridad.
- Debe abarcar la mayor cantidad de casos posibles en los ámbitos que la definen.

Además de estas consideraciones, las políticas de seguridad deben alinearse con la misión y visión de la organización, por lo cual se diseñan de forma que puedan ser aplicadas por largos períodos de tiempo sin requerir mayores cambios. Es normal que las revisiones de políticas se hagan sólo cuando se cumplen algunas de estas condiciones:

- Ha pasado un período de tiempo largo desde su última revisión. Normalmente en el orden de los años (por ejemplo entre cada 3 y 5 años).
- Hubo un incidente de seguridad que evidenció que la política no es efectiva en cierto escenario y debe ser reformulada para enfrentar mejor futuros riesgos.
- Hubo un cambio relevante en la misión y visión de la organización y se debe refrescar la política para adaptarse al cambio en las operaciones.

Las políticas de seguridad deben ser respetadas por todos los miembros de la organización, por esta razón se hace importante que los encargados de la dirección y operaciones estén involucrados en el proceso, aprueben estas políticas y ayuden a su cumplimiento durante las operaciones habituales.

2. Presentar el concepto de directiva de seguridad al grupo:

> Directiva de seguridad: Conjunto de reglas específicas que son implementadas por el equipo de trabajo y sus aliados relevantes para implementar las políticas de seguridad en el trabajo diario. Estas directivas pueden ser más concretas en el uso de herramientas y equipos específicos, y pueden cambiar en el tiempo con más frecuencia.

- Este concepto puede ser planteado como la unión de varias ideas: Son reglas puntuales.
- Su misión es ayudar al cumplimiento de las políticas.
- Se relacionan con los procesos del día a día.

Dado que las directivas de seguridad son más dependientes de tecnologías y prácticas habituales, están pensadas para ser revisadas y cambiadas mucho más frecuentemente que las políticas, como guía general se sugiere revisar las directivas cuando se cumple alguna de estas condiciones:



- Ha pasado una cantidad de tiempo en donde algunas prácticas de seguridad pudieron ser cuestionadas o mejoradas gracias a descubrimientos o actualizaciones. Por ejemplo, cuando se descubre una vulnerabilidad crítica en una herramienta o cuando sale un nuevo producto que mejora las condiciones de los procesos de la organización y quiere ser implementado. Normalmente estos tiempos se miden en meses (por ejemplo entre cada 3 a 12 meses).
- Hubo cambios en las políticas de seguridad relacionadas, incluyendo cambios producto de incidentes de seguridad que afectan la política en cuestión.

Las directivas de seguridad tienen un lenguaje instruccional claro, especificando acciones concretas a tomar en ciertos escenarios, por ejemplo:

- X pieza de información se transmite a través de estos canales: ...
- No se permite utilizar Y dispositivo para almacenar información de sensibilidad alta.
- Z pieza de información puede transmitirse por W canal bajo las siguientes condiciones: ...

Como diferencias notables entre las políticas y directivas de seguridad están:

- Su alcance: las políticas son generales y las directivas son específicas.
- Su dependencia: las directivas de seguridad son una parte de las políticas de seguridad.
- Su evolución en el tiempo: generalmente las políticas de seguridad cambian en el orden de los años, las directivas de seguridad en el orden de los meses.

En muchos de los marcos de referencia de seguridad de la información, el concepto de directiva de seguridad es representado bajo otros documentos o nombres, pudiendo generar confusión al consultar otro tipo de literatura. En este caso, lo más importante para adaptar este concepto es entender que se trata de instrucciones claras para ejecutar una acción determinada cumpliendo con las políticas de seguridad, en este manual se abstrae el concepto de directiva para armar un modelo que sea de rápida comprensión y facilitación para los grupos objetivo.

## _Cierre de la actividad

En esta actividad de capacitación se exploraron de una manera rigurosa los conceptos de política y directiva de seguridad, los cuales permitirán avanzar de forma efectiva en las siguientes actividades.

## _Referencias


R11 Information Security Policy Templates | SANS Institute

R12 Introduction to Security Policies, Part One: An Overview of Policies | Symantec

R13 Information Security Handbook: A Guide for Managers | NIST


# 02_ Política de protección de información

Tiempo estimado: 60 min

## _Justificación

Uno de los aspectos medulares de cualquier organización es la manipulación de información, ya que cualquier proceso que se realice puede ser abstraído a la generación, procesamiento, almacenamiento y publicación de información. En el caso de organizaciones que realizan activismo o documentación en el área de Derechos Humanos existe una variedad importante de tipos de información cuyo compromiso puede desencadenar consecuencias negativas para la organización, sus miembros o actores relacionados. La idea de desarrollar una política de protección de información es establecer una serie de lineamientos que ayuden a tratar cada pieza de información de la forma más adecuada posible y acorde a la sensibilidad de la misma.

## _Datos de entrada

- Mapa de datos desarrollado en la sección Mapeo y clasificación de información
- Mapa de flujos de datos desarrollado en la sección Mapeo de flujos de información
- Plantilla 1: Política de protección de información, abierta en un equipo para alimentarla en el transcurso de la actividad.

## _Conceptos Asociados

- Niveles de sensibilidad de información: Escala por la cual se establece que tanto una pieza de información debe ser protegida.
- Principio del minímo privilegio: Propone que la información debe ser accesible solo a personas que necesitan usarla dentro de sus procesos habituales.
- Responsables de la información: Son aquellas personas con competencias directas en la manupulación de la información.
- Disposición de información: Técnicas utilizadas para deshacerse de piezas de información una vez que han cumplido su vida útil o que debe ser destruida por regulaciones y/o seguridad.



## _Políticas a desarrollar

Política de Protección de Información: a desarrollarse en esta actividad, abstrae contenidos existentes en las siguientes políticas descritas en marcos de referencia estandarizados:

- Política de clasificación de información: Define criterios por los cuales se determina el nivel de sensibilidad de la información manejada y líneas estratégicas de manejo de esta información a los niveles de sensibilidad propuestos. También define usualmente los responsables del manejo y resguardo de las piezas de información trabajadas en la organización.
- Política de retención de datos: Define entre otras cosas el tiempo que la organización puede conservar cierto tipo de información sensible, cómo disponer de ella, cuándo se desincorpora, en qué dispositivos, qué prácticas de seguridad deben aplicarse a cada tipo de información sensible, y cómo se procesa la información sensible de acuerdo a regulaciones legales y mejores prácticas.
- Política de acceso a datos: Esta define las piezas de información que pueden ser accedidas y manipuladas por los distintos grupos y personas de la organización, en función de disminuir las posibilidades de compromiso de la misma y de hacer más eficientes los flujos de información dentro de los procesos de la organización.

## _Preguntas guía

1. ¿Cuál es el alcance de la política propuesta?
2. ¿Qué niveles de sensibilidad tiene la información manejada por la organización y cómo se describen?
3. ¿Cómo se puede clasificar cualquier pieza de información en los niveles de sensibilidad propuestos?
4. ¿Quiénes son los responsables del resguardo de la información?
5. ¿Quiénes deben tener acceso a la información y quienes no?
6. ¿Qué medidas se deben tomar para manipular información según su nivel de sensibilidad? (Plantear conceptos clave)
7. ¿Qué herramientas, prácticas y dispositivos específicos se deben emplear para manipular la información según su nivel de sensibilidad?

### 1. Alcance de la política

En esencia, el alcance asociado a esta política abarca dos aspectos:

Las personas del equipo afectadas: Pudiendo abarcar por ejemplo todos los miembros del equipo, sólo algunos de ellos (equipo de periodismo de investigación, encargados de manejar denuncias, etc.), personas puntuales o incluso todos los miembros de la organización y cualquier aliado externo que colabore con el equipo en ciertos temas.

Los tipos de datos considerados: Teniendo como opciones sólo ciertos tipos de información manejados por la organización o todas las piezas de información manejadas por el grupo. Este ejercicio está diseñado para considerar el segundo caso, sin embargo, se puede manejar como mejor juzgue el grupo siempre que se pueda desarrollar la actividad con fluidez.
Se propone discutir ambos aspectos y colocar el resultado de la discusión en la sección (1) de la plantilla.

## 2. Niveles de sensibilidad de la información manejada.

¿Qué niveles de sensibilidad tiene la información manejada por la organización y cómo se describen? ¿Cómo se puede clasificar cualquier pieza de información en los niveles de sensibilidad propuestos?

1. Revisar la matriz de consecuencias de la actividad de mapeo y clasificación de información ya sea en físico o transcrita en digital.

2. Introducir algunos tipos de información en esquemas de clasificación utilizados habitualmente en seguridad de la información y proponer mantenerse con los niveles de impacto desarrollados.
   - Frecuentemente se emplean las clasificaciones de información pública/confidencial/secreta o pública/interna/confidencial/regulatoria entre otras, tomando en cuenta el daño que puede generar su compromiso.
     En términos de nuestra metodología, los mismos niveles de impacto propuestos en secciones anteriores pueden llenar este espacio y por eso se proponen por motivos de simplicidad.

3. Unificar en una sola celda de tabla el contenido de cada fila por nivel de impacto desarrollado y vaciar esta información en la sección (2) de la plantilla como muestra el gráfico.



| Nivel de Impacto | Descripción<br>Su compromiso puede generar |
|---|---|
| Bajo | • Pérdida de servicios públicos en la oficina<br>• Destrucción o pérdida de equipos<br>• Monitoreo administrativo excesivo<br>• Pérdidas pequeñas de equipo o dinero |
| Medio | • Destrucción de oficina<br>• Cargas de trabajo o estrés inmanejables<br>• Allanamientos<br>• Juicios<br>• Prohibición de salida del país de un miembro<br>• Multas<br>• Perdidas importantes de equipos o dinero<br>• Pérdida de cuentas sociales de la organización o sitios web |
| Alto | • Filtrado de datos de denunciantes<br>• Muerte de beneficiario o miembro del equipo<br>• Eventos traumáticos a personas<br>• Arrestos<br>• Pérdida de figura legal<br>• Quiebra de la Organización<br>• Pérdida de cuentas de correo |

Grafico 14 Niveles de impacto en la información

### 3. Responsables de la información

> ¿Quiénes son los responsables del resguardo de la información?

Cuando se maneja información con diferentes niveles de sensibilidad es importante garantizar que hay medidas de seguridad puestas en marcha para proteger esta información, y se vuelve relevante saber quiénes son los responsables de implementar y mantener las medidas de seguridad propuestas. Aunque marcos de referencias estandarizados proponen varias figuras relativas a la responsabilidad sobre la información, se propone sólo emplear la figura del custodio de información. Dependiendo de las necesidades y dinámicas de la organización hay varias aproximaciones a la determinación de quiénes son los custodios de la información, algunos ejemplos son:

- Las personas que generan los objetos de información.
- Coordinadores de departamentos o áreas asociadas a los objetos de información.
- Las personas que en cada momento manipulan la información.
- Personas específicas designadas caso a caso.
- Otros criterios de asignación.

La propuesta es presentar estas opciones y discutir cual de ellas aplica mejor para la organización y dejarlo por escrito en la sección (3) de la plantilla.

### 4 Restricción base de acceso a la información

> ¿Quiénes deben tener acceso a la información y quienes no?

En el marco del establecimiento de políticas de protección de la información, es importante considerar el control del acceso a la misma por parte del equipo, esto se logra teniendo listas o reglas de control de acceso que determinan quiénes pueden acceder a cada tipo de información y quienes no. Usualmente estas consideraciones se incluyen en una Política de acceso a datos, sin embargo, este tipo de políticas se fundamentan en el principio del minímo privilegio, en donde se propone que sólo las personas que necesitan manipular cierta información sean capaces de acceder a ella por regla, minimizando las posibilidades de compromiso de la misma.



La primera premisa que se quiere validar con el grupo es si ellos estarían de acuerdo con seguir formalmente este principio, se espera que el grupo esté de acuerdo pero vale la pena explorar cualquier escenario en donde se dificulte. En estos casos se debe dejar claro que las probabilidad de compromiso de la información puede subir considerablemente. El principio de minímo privilegio se tiene escrito por defecto en la sección (4) de la plantilla.

### 4a. Políticas de control de acceso (opcional)

En el caso en que la organización maneje información muy sensible, se muestre interesada en profundizar en el control de acceso a información y se disponga del tiempo, se puede desarrollar una primera versión de una matriz de control de acceso. En la sección (4a) de la plantilla se encuentra un ejemplo de matriz en donde se colocan como columnas diferentes departamentos, áreas, coordinaciones o inclusive cargos específicos dependiendo de la estructura y dinámicas de la organización, y como filas piezas de información con niveles de sensibilidad altos, y básicamente se describe qué áreas o personas pueden acceder a qué piezas.

| Información | Director | Denuncias | Comunic. | Finanzas | IT |
|---|---|---|---|---|---|
| Datos de denunciantes | | X | | | |
| Informes | X | X | X | | |
| Datos de donantes | X | | | X | |
| Respaldo de artículos | | | X | | X |
| Grabaciones de fuentes | | | X | | |

Grafico 15 Matriz de control de acceso a datos

## 5. Directivas generales de manipulación de información

¿Qué medidas se deben tomar para manipular información según su nivel de sensibilidad?

Usando la matriz desarrollada en la actividad de flujos de información se pueden recopilar los criterios generales descritos para cada nivel de impacto y describirlos en la sección (5) de la plantilla.

Es importante que en esta sección se evite escribir herramientas o servicios específicos, sino las características de seguridad asociadas, que permitan en el caso de cambiar una herramienta, tener el criterio para seleccionar una nueva que cumpla con las mismas o mejores prestaciones. Por ejemplo: no colocar para comunicaciones Signal sino Servicios de chat con cifrado de extremo a extremo.

| Nivel de Impacto | Consideraciones |
|---|---|
| Medio | Se debe comunicar en servicios cifrados<br>No debe almacenarse en equipo usados por visitantes o pasantes<br>Su envío a actores externos debe ser autorizado por el custodio de la Información<br>Sólo deben existir copias físicas bajo llave |
| Alto | Se comunica sólo en canales cifrados de extremo a extremo<br>Sólo se almacenan en dispositivos con cifrado de disco<br>Su envío a actores externos está prohibido<br>No deben existir copias físicas |

Grafico 16 Consideraciones generales por nivel de impacto



## 6. Directivas específicas de manipulación de información.

¿Qué herramientas, prácticas y dispositivos específicos se deben emplear para manipular la información según su nivel de sensibilidad?

De forma similar al paso anterior, para cada nivel de impacto o sensibilidad se recopilarán los dispositivos, otros lugares de reposo de la información y canales de comunicación que se seleccionaron para cada nivel, y así colocarlos en las tablas de la sección (6) de la plantilla como se indica. Se deja el espacio para colocar las consideraciones necesarias que se necesiten cumplir en cada caso si aplica.

Por simplicidad, si la organización y el facilitador lo consideran conveniente, se pueden considerar sólo los niveles de impacto más altos, dado que los niveles más bajos pueden requerir más tiempo y esfuerzo para llenar la información solicitada en la plantilla, en ese caso las tablas para niveles bajo y medio se pueden borrar de la plantilla.

| Para Información de sensibilidad alta | |
|---|---|
| Dispositivo/canal de comunicación | Consideraciones |
| Correo electrónico | Sólo con PGP o entre cuentas Protonmail |
| PCs | Sólo en aquellas con cifrado de disco |
| Teléfonos celulares | Estrictamente prohibido |

| Para Información de sensibilidad media | |
|---|---|
| Dispositivo/canal de comunicación | Consideraciones |
| Chats | Signal, Wire, Chats secretos de Telegram |
| Teléfonos celulares | Con cifrado de dispositivos y contraseña |
| Correo electrónico | Entre cuentas Gmail |
| PCs | Usando cifrado de archivos de Veracrypt |
| Memorias USB | Estrictamente prohibido |
| Soportes físicos | En caja fuerte de oficina |

Grafico 17 Directivas de seguridad por nivel de impacto

## _Aspectos excluidos de la política

- Tiempo de vida de la información: donde se especifique por cuánto tiempo la organización retendrá ciertos tipos de información y qué tipo de procesamiento se necesitará realizar antes de desincorporarlos o borrarlos.
- Disposición de la información: cómo se debe eliminar la información según su tipo de sensibilidad, con la intención de evitar la reconstrucción de esta información o el rastreo de la existencia de los datos.
- Detalle de riesgos asociados a esta política: en donde se elabore en qué tipo de riesgos se están atacando con el cumplimiento de esta política.
- Responsabilidades puntuales: donde se pueden especificar responsabilidades que escapan de ser custodio de la información y pueden ser relevantes para la organización.
- Plan de capacitación en los conceptos, técnicas y herramientas propuestos en la política.

## _Referencias

R14 Information Classification Policy | ISO



# 03_ Política de uso aceptable de equipos Cuentas y contraseñas

Tiempo estimado: 60 min

## _Justificación

Actualmente la mayoría de organizaciones independientemente del campo que desarrollan utilizan tecnología dentro de sus procesos, esta tecnología tiene inevitablemente vulnerabilidades y es propensa a fallar o ser abusada. Tomando esto en cuenta, la idea de esta política es brindar lineamientos de uso seguro a los puntos de entrada de cualquier persona con la tecnología tanto a nivel de dispositivos como de servicios en internet para proteger a la organización de la mejor manera posible. Específicamente se describen medidas de seguridad básicas en el uso de dispositivos móviles o de escritorio, de servicios ampliamente usados como el correo electrónico y redes sociales, en la construcción y gestión de contraseñas y otros medios de autenticación dentro de la organización.

## _Datos de entrada

- Política de protección de información.
- Plantilla 2: Política de uso aceptable de equipos, cuentas y contraseñas disponible en físico o en digital para ser llenada en el transcurso de la actividad.

## _Conceptos asociados

- Actualizaciones de software: Parches de código de algunas partes del sistema operativo que buscan mejorar funcionalidades y corregir nuevas vulnerabilidades de seguridad.
- Cifrado: Capacidad de transformar un mensaje en algo ininteligible para otros y poder revertirlo al contenido original por quienes queremos que tengan acceso a la información.
- Cifrado de disco o de dispositivo: Proceso que permite cifrar todo el contenido del disco duro de un equipo de tal forma que sólo sea accesible y usable cuando al encender se introduzca una contraseña u otro método de autenticación que aplique.
- Software pirata: Cualquier software que se instale por fuera de los canales oficiales sin pagar su valor de licenciamiento.
- Malware: Cualquier software malintencionado que ejecute acciones en un equipo sin autorización de su propietario o responsable.

- Phishing: Una serie de ataques que utilizan la suplantación de identidad como un mecanismo para lograr que un usuario realice una acción perjudicial para si mismo, los equipos que utiliza, los datos que almacena y su red.
- Contraseña: Secuencia de caracteres secretos que son usados para ingresar a un servicio o dispositivo.
- Credenciales: la unión de nombres de usuario y contraseñas, son usadas para identificar a un usuario en un servicio y comprobar que es quien dice ser. Estas credenciales cada vez más frecuentemente incluyen otros factores como aspectos biométricos y códigos temporales de seguridad.
- VPN (Red Privada Virtual): Tecnología que permite tratar equipos que pueden estar en ubicaciones remotas como parte de una red interna, frecuentemente utilizados por organizaciones para unir en una sola red a varios equipos en ubicaciones dispersas. Una aplicación particular de esta tecnología permite a usuarios particulares cifrar el contenido de sus conexiones a internet entre sus dispositivos y lugares considerados seguros antes de llegar a internet, generalmente se utilizan para proteger el tráfico de vigilancia y acceder a contenidos bloqueados.
- Tor: Infraestructura de red que permite navegar en internet redireccionando los datos por puntos aleatorios alrededor del mundo. Estos datos viajan cifrados y el sistema está diseñado para brindar anonimato y protección contra la vigilancia.
- URL: Secuencias de caracteres que permiten ubicar recursos en internet, significa Localizador de Recursos Universal. http://sdamanual.org es un ejemplo de URL.
- Antivirus: Software que analiza archivos en busca de piezas de malware conocidas, generalmente tienen una base de datos de amenazas previamente identificadas, entonces compara archivo por archivo con esta base de datos para detectar posibles coincidencias.
- PGP/GnuPG/GPG: Conjunto de estándares y tecnologías que permiten aplicar principios de cifrado asimétrico (el cual se considera mucho más seguro que las técnicas tradicionales) a mensajes y archivos en equipos computacionales. Generalmente se usa como una estrategia avanzada de seguridad dado el esfuerzo que requiere su implementación y el alto nivel de seguridad que provee.
- Administrador de contraseñas: Software que permite almacenar contraseñas previamente diseñadas y recuperarlas cuando se necesiten. Generalmente permiten generar contraseñas con mucha mayor longitud y complejidad dado que no es necesario recordarlas al momento de su uso.
- Autenticación en 2 factores o autenticación en 2 pasos: Técnica de autenticación basada en solicitar para ingresar a un servicio además de una contraseña, otro elemento relacionado con algo que posee físicamente el usuario, como por ejemplo un teléfono celular, una tarjeta con códigos, etc.



## _Políticas a desarrollar

La Política de uso aceptable, cuentas y contraseñas: a desarrollarse en esta actividad, abstrae contenidos existentes en las siguientes políticas descritas en marcos de referencia estandarizados:

- Política de uso aceptable de equipos: Define condiciones básicas para usar de forma segura computadoras, teléfonos y otros equipos móviles. usualmente trata temas como contraseñas de acceso, bloqueo de equipo, cifrado y reporte de incidentes entre otros.
- Política de uso aceptable de internet: Establece algunos principios de seguridad relacionados al uso de navegadores y otras aplicaciones que se conectan a internet en función de proteger los equipos usados y la información contenida en estos.
- Política de uso aceptable del correo electrónico: Establece lineamientos específicos al uso del correo electrónico. En principio busca disminuir los ataques de phishing, de exfiltración de información y las infecciones de equipos por malware, también puede incluir lineamientos sobre los propósitos con los que se usa el correo, lenguaje y otros aspectos relevantes para el buen uso del correo electrónico en la organización.
- Política de uso aceptable de redes sociales: Determina medidas de seguridad a tomar en el uso y administración de redes sociales de la organización. Normalmente tiene un conjunto de reglas generales y otras específicas por cada servicio de interés.
- Política de cuentas y contraseñas: En esta política se establecen un conjunto de reglas que rigen la creación, el uso y mantenimiento de contraseñas en diferentes servicios y de acceso a dispositivos, en caso de que la organización maneje algunos sistemas propios, puede especificar lineamientos de administración de contraseñas para sus usuarios. En ocasiones, esta política también considera aspectos diferentes a las contraseñas, como biometría u otros factores de autenticación.

## _Preguntas guía

1. ¿Cuál es el alcance de la política propuesta?
   - ¿A quiénes afecta esta política?
   - ¿Incluye los equipos propiedad de la organización o cualquiera que se use para trabajar en esta?
   - ¿Incluye computadoras o también dispositivos móviles?
   - ¿Qué servicios de correo electrónico y redes sociales incluye?
2. ¿Quiénes son responsables de implementar y mantener las medidas de seguridad en los equipos?
3. ¿Cuáles son las medidas de seguridad generales y directivas en el manejo de equipos?
4. ¿Cuáles son las consideraciones de seguridad generales al usar cualquier canal de comunicación?

5. ¿Cuáles son las medidas de seguridad generales al usar internet?
6. ¿Cuáles son las consideraciones de seguridad generales a seguir en la gestión de cuentas de usuario?
7. ¿Qué políticas de seguridad se deben poner en práctica con los servicios autogestionados por la organización?
8. ¿Cuáles son los lineamientos de seguridad que se deben seguir al gestionar cuentas en servicios hospedados por terceros?
   - Correo electrónico
   - Redes Sociales
   - Otros servicios
9. ¿Qué aspectos de seguridad deben ser considerados alrededor de la gestión de contraseñas y otros mecanismos de autenticación?

## 1. Alcance de la política

En resumen, el alcance asociado a esta política abarca los siguientes aspectos:

- A qué personas impacta esta política: generalmente se incluyen todos los miembros de la organización y aliados que trabajen en proyectos específicos si aplica.
- Qué equipos impacta la política:
  - Si sólo incluye equipos que son propiedad de la organización o si también incluye a los equipos propiedad de los miembros de la organización usados con fines profesionales (modelo de trabajo Trae tu propio equipo o Bring Your Own Device - BYOD en Inglés).
  - Si incluye computadoras y/o teléfonos y otros equipos móviles.
- Qué tipo de servicios digitales abarca: si incluye correo electrónico, uso general de internet, redes sociales o cualquier otro servicio relevante para la organización. Una opción válida también puede ser todos los servicios que se utilicen para el trabajo en la organización.

Para esta sección se debe discutir, modificar y aprobar el contenido de la sección (1) de la plantilla de política de uso aceptable de equipos, cuentas y contraseñas. Es muy importante que las disposiciones que se establezcan en esta y las demás políticas desarrolladas estén alineadas con el resto, en este caso con la política de protección de información la cual puede brindar ayuda al momento de decidir lineamientos específicos.

## 2. Responsabilidad sobre los equipos

> ¿Quiénes son responsables de implementar y mantener las medidas de seguridad en los equipos?

Discutir, modificar y aprobar el contenido de la sección (2) de la plantilla de política de uso aceptable de equipos, cuentas y contraseñas que trata sobre la propiedad de los equipos y las responsabilidades de uso de los mismos y sobre el reporte de incidentes.



La variación más notable en este paso depende de si la organización tiene sus propios equipos, todos los equipos son propiedad de los miembros de la organización (BYOD) o una mezcla de ambas modalidades. En la plantilla se encuentran varios ejemplos que puede ser reducidos al caso particular de la organización ejecutando la actividad.

## 3. Uso general de equipos

> ¿Cuáles son las medidas de seguridad generales y directivas en el manejo de equipos?

Discutir, modificar y aprobar el contenido de la sección (3) de la plantilla de política de uso aceptable de equipos, cuentas y contraseñas. Algunos de los aspectos más importantes tratados en esta sección son:

- Medios de autenticación para equipos como contraseñas o biometría.
- Bloqueo de equipos cuando se dejan desatendidos.
- Compartición de credenciales de acceso a equipos.
- Actualizaciones de sistema operativo.
- Uso de software pirata.
- Consideraciones contra la infección con malware.
- Cifrado de disco.
  - En computadoras.
  - En teléfonos celulares y otros equipos móviles.
- Uso de equipos para fines diferentes al trabajo de la organización.
- Uso de Antivirus y Antimalware.

## Directivas de uso aceptable de equipos

Discutir, modificar y aprobar la sección de directivas que se encuentra en la sección (3) de la plantilla de política correspondiente. Es ideal que el grupo tenga un conocimiento previo de temas puntuales de seguridad, siendo el caso óptimo tener esta discusión posterior a la realización de un taller de seguridad digital, así a medida que se cubra cada aspecto trabajado en este manual, se pueda discutir cómo se quiere implementar este concepto o herramienta a la política correspondiente. Como ejemplos en la plantilla que pueden ser utilizados como aparecen, editados o eliminados se encuentran, entre otros:

- El uso obligatorio de contraseñas de usuario en las computadoras y teléfonos celulares usados para tratar temas sensibles de la organización. Estas contraseñas deben cumplir con las políticas de contraseñas al final de este mismo documento.
- El uso obligatorio de protectores de pantalla que bloquean los usuarios en computadoras y celulares después de cierto tiempo de inactividad.

- La implementación de cifrado de sistema: en el caso de los dispositivos móviles frecuentemente esta característica viene activada por defecto y en el caso de computadoras puede requerir tiempo, conocimiento y esfuerzo especial para implementar un cifrado efectivo de disco. En este aspecto es frecuente la concentración de esfuerzos en aquellos equipos que manejan información de alta sensibilidad, en planes de mantenimiento de equipos que considere la configuración de este cifrado de disco o en el uso de sistemas operativos que facilitan por diseño el cifrado de sistema.
- La política de actualizaciones de sistema operativo: Generalmente se considera como el mínimo necesario hacer actualizaciones de seguridad automatizadas, desde ese punto en adelante se puede ajustar la política a cada organización según sus necesidades.
- Uso de software antivirus y antimalware, pudiendo especificar software específico aprobado o criterios de selección.

## 4. Uso general de equipos

> ¿Cuáles son las consideraciones de seguridad generales al usar cualquier canal de comunicación?

Discutir, modificar y aprobar el contenido de la sección (4) de la plantilla correspondiente. Algunos de los aspectos más importantes tratados en esta sección son:

- El manejo de información de alta sensibilidad a través de estos canales y hacia actores externos a la organización.
  Uso de los equipos para fines distintos al trabajo relacionado a la organización.
- La actitud de los integrantes de la organización como representantes de la misma al usar los canales de comunicación oficiales. Actitudes respecto a la discriminación, acoso, spam, etc. en los canales de comunicación utilizados para fines organizacionales.
- Disposiciones sobre el uso de los equipos para realizar acciones que violen los derechos de propiedad intelectual y copien o distribuyan material protegido por derechos de autor.

## 5. Directivas de uso general de internet

> ¿Cuáles son las medidas de seguridad generales al usar internet? Discutir, modificar y aprobar el contenido de la sección (5) de la plantilla correspondiente. En caso de que alguna consideración no aplique a la organización se puede eliminar sin problemas. Algunos de los aspectos más importantes tratados en esta sección son:



- El uso de herramientas de circunvención y anonimato en internet al usar los equipos como Redes Privadas Virtuales (o VPNs en Inglés), Tor u otro tipo de herramientas afines. Normalmente estas medidas van asociadas a niveles de sensibilidad de la información manejada. Dado que es una directiva se puede ser específico en herramientas puntuales aprobadas o criterios de selección.
- La prohibición de actividades que deterioren injustificadamente la calidad de la conexión (por ejemplo descargas de torrents o streaming de contenidos no relacionados al trabajo).

### Estrategias contra la suplantación de identidad

Dado que los ataques más frecuentes a organizaciones en la actualidad están relacionados en gran medida a ataques de suplantación de identidad (o phishing en Inglés), es importante especificar estrategias claras para enfrentar estos riesgos. Se propone revisar en la sección (5) de la plantilla en uso la sección correspondiente y discutir, editar, agregar y aprobar algunas de las estrategias propuestas, relacionadas a temas como:

- El conocimiento por toda la organización de los canales de comunicación oficiales de los actores relevantes relacionados (por ejemplo proveedores, personal, instituciones públicas) y evitar cualquier comunicación o intercambio de información sensible por canales diferentes. (direcciones de correo electrónico, cuentas en redes sociales y números telefónicos entre otros)
- El manejo de comunicaciones que solicite información sensible como credenciales, información bancaria y personal además del desarrollo de una serie de indicadores que ayuden a detectar posibles casos de suplantación de identidad.
- El desarrollo de reglas de manejo de archivos adjuntos sospechosos.

## 6. Gestión de cuentas

> ¿Cuáles son las consideraciones de seguridad generales a seguir en la gestión de cuentas de usuario?

- Obligatoriedad de cuentas individuales o compartidas.
- Responsabilidad por el uso de cuentas propias.
- Implementación del principio del mínimo privilegio en la creación y configuración de cuentas de usuario.
- Manejo de mecanismos de recuperación de cuentas.

### 7. Manejo de cuentas en servicios autogestionados (Sistemas internos, websites hosteados, servidores, etc.)

> ¿Qué políticas de seguridad se deben poner en práctica con los servicios autogestionados por la organización?

Discutir, modificar y aprobar el contenido de la sección (7) de la plantilla de política de uso aceptable de equipos, cuentas y contraseñas. Algunos de los aspectos más importantes tratados en esta sección son:

- Concepto de administradores: quién crea, monitorea, controla y elimina una cuenta y bajo qué circunstancias?.
- Quién autoriza la creación de las cuentas.
- Evitar cuentas administrativas para uso diario.
- Acuerdos de no divulgación (NDA).
- Roles de acceso a sistemas.

### 8. Directivas sobre el manejo de cuentas en servicios de terceros (Correos electrónicos, redes sociales, servicios de colaboración, etc.)

> ¿Cuáles son los lineamientos de seguridad que se deben seguir al gestionar cuentas en servicios hospedados por terceros?

Discutir, modificar y aprobar el contenido de la sección (8) de la plantilla de política de uso aceptable de equipos, cuentas y contraseñas. Algunos de los aspectos más importantes tratados en esta sección son:

#### Sobre el correo electrónico

- Publicación de opiniones personales en los correos.
- Apertura de archivos adjuntos sospechosos.
- Generación de correo no deseado o malintencionado.
- En caso de requerirlo en la política de protección de datos considerar cifrado de correos.

#### Sobre otros servicios de terceros

- Quiénes manejan las credenciales de acceso.
- Uso de herramientas de publicación colaborativa que protegen las credenciales de las cuentas en redes sociales.
- Uso de gestores de contraseñas.
  En caso que aplique monitoreo de cuentas falsas.

#### Para cada servicio específico

- ¿Qué características se pueden configurar además de las presentes en la política general?

Ejemplo: Facebook

- Uso de páginas vs usuarios o grupos.
- Gestión de administradores.
- Notificaciones de seguridad.
- Autenticación en dos factores.
- Contactos de emergencia.

Ejemplo: Twitter

- Vinculación de número telefónico a la cuenta.

### 9. Políticas y directivas de contraseñas y autenticación

> ¿Qué aspectos de seguridad deben ser considerados alrededor de la gestión de contraseñas y otros mecanismos de autenticación?

Discutir, modificar y aprobar el contenido de la sección (4) de la plantilla correspondiente. Algunos de los aspectos más importantes tratados en esta sección son:

- El principio básico de responsabilidad directa en el uso de las cuentas, dispositivos o servicios con contraseña a su cuidado.
- Medidas de seguridad para la creación de contraseñas, en pasos posteriores se definirán estas medidas en detalle.
- Prácticas generales de seguridad para contraseñas.
  - Repetición de contraseñas.
  - Existencia de copias físicas.
  - Recordar contraseñas en exploradores.
  - Uso de administradores de contraseñas.
  - Compartición de contraseñas.
- Propuestas de directivas para contraseñas y autenticación.
  - Longitud.
  - Complejidad.
  - Diccionario.
  - Contenidos a evitar en la construcción de la política.
  - Autenticación en varios factores.
  - Uso de administradores de contraseña.
  - Contraseñas de acceso en equipos móviles..

#### Aspectos excluidos en la política

- Gestión remota de equipos.
- Monitoreo y auditoría del cumplimiento de las políticas de seguridad en equipos.
- Prohibición explícita del monitoreo de red, análisis de puertos y uso de honeypots y honeynets.
- Prohibición explícita de ejecución de cualquier tarea ilegal, por ejemplo ataques de denegación de servicio (DoS y DDoS) y bloqueo en el acceso a recursos a otros usuarios de forma injustificada.

## _Referencias


R15 Acceptable use policy template I SANS Institute

R16 Sample Acceptable Usage Policy I getsafeonline.org

R17 Email policy template I Sans institute

R18 Password Protection Policy template I SANS Institute

# 04_ Política de limpieza de escritorio

Tiempo estimado: 20 min

## _Justificación

En cualquier tipo de organización, independientemente del uso que hagan de la tecnología, es normal que se tengan grandes cantidades de información de alta sensibilidad en físico, además, cuando hablamos de espacios de trabajo los equipos utilizados para almacenar y manipular información pasan a ser objetos físicos de interés para aquellos que quieran comprometer los datos de la organización. La idea detrás de esta política es establecer un conjunto de estrategias que permitan asegurar tanto la información en físico como la integridad de los equipos que se utilizan en los espacios de trabajo de la organización. Esta política es una de las más vinculadas al día a día del equipo ya que considera actividades que deben realizarse durante toda la jornada de trabajo.

## _Datos de entrada

- Plantilla 3: Política de limpieza de escritorio disponible en físico o en digital para ser llenada en el transcurso de la actividad.

## _Políticas a desarrollar

En principio, la Política de limpieza de escritorio o (Clean desk policy en Inglés) se encuentra de forma explícita en la mayoría de los marcos de referencia utilizados en varias organizaciones.

## _Preguntas guía

- ¿Cuál es el alcance de esta política?
- ¿Qué medidas de deben tomar en los espacios de trabajo en la organización?
- ¿Cómo se debe manejar la información en físico en los espacios de trabajo?
- ¿Cómo se debe disponer de la información física una vez que debe ser descartada?

### Alcance de la política

En resumen, el alcance asociado a esta política, disponible en la sección (1) de la plantilla de política de limpieza de escritorio abarca los siguientes aspectos:

- Espacios de trabajo afectados por esta política.
- Personal afectado por esta política.



### Medidas en espacios con equipos de trabajo

> ¿Qué medidas de deben tomar en los espacios de trabajo en la organización? Discutir, modificar y aprobar el contenido de la sección (2) de la plantilla correspondiente. Algunos de los aspectos más importantes tratados en esta sección son:

- Pasos particulares a seguir al final de la jornada laboral.
- Manejo de equipos desatendidos durante la jornada de trabajo.
- Uso de mecanismo de resguardo físico para los dispositivos en los espacios de trabajo.

### Manejo de información en físico en los espacios de trabajo

> ¿Cómo se debe manejar la información en físico en los espacios de trabajo?

Discutir, modificar y aprobar el contenido de la sección (3) de la plantilla correspondiente. Algunos de los aspectos más importantes tratados en esta sección son:

- Procesos a seguir al final del día para mantener los espacios de trabajo libres de información sensible.
- Manejo de archivadores u otros mecanismos de resguardo de información en físico.
- Manejo de llaves de muebles y cajas de seguridad.
- Existencia de información sensible en espacios de trabajo.
- Manejo de papeles en impresoras.
- Manejo de información en pizarras y carteleras.
- Manejo de dispositivos de almacenamiento digital portátil.

### Disposición de información en físico

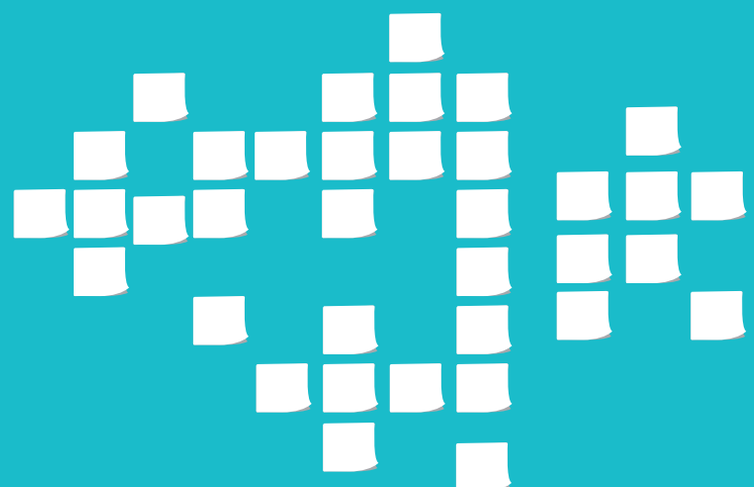
> ¿Cómo se debe disponer de la información física una vez que debe ser descartada?

Discutir, modificar y aprobar el contenido de la sección (4) de la plantilla correspondiente. Algunos de los aspectos más importantes tratados en esta sección son:

- El uso de equipamiento o técnicas para hacer ininteligible la información física de la que se desea disponer.
- Lugares seguros para depositar la información en físico después de haber sido procesada para su disposición.

## _Referencias

R19 Clean Desk Policy template | SANS Institute



# 03_ Modelo de Amenazas y Procedimientos

## _ Conceptos

- **Amenaza:**
  Posible evento o hecho con consecuencias negativas.
- **Riesgo:**
  Posibilidad de que una amenaza se concrete.
- **Vulnerabilidad:**
  La condición de debilidad o la inexistencia de una medida que proteja algo de una amenaza.
- **Incidente de seguridad:**
  Cualquier violación a las políticas de seguridad o vulneración de un recurso determinado.
- **Procedimiento de seguridad:**
  Una serie de pasos que se pueden seguir en orden para afrontar un incidente de seguridad.
- **Plan de sucesión:**
  Listado elaborado previo a un incidente de seguridad en donde se especifican los responsables de cumplir el procedimiento de seguridad y quienes los suplirían en el caso de que los primeros no estén disponibles.
- **Plan de comunicaciones:**
  Compilación de contactos que la organización desea hacer ante un incidente de seguridad determinado. Incluyendo con qué actores se establecerá comunicación, qué integrantes de la organización son los responsables de estas comunicaciones y qué se debe comunicar.
- **Evidencia:**
  Cualquier elemento físico o digital que pueda ser usado para futuras investigaciones y a la vez pueda ser considerado prueba para acciones legales y/o penales.



## 01_ Matriz de Riesgo

Tiempo estimado: 120 min

### _Justificación

La idea de esta actividad es introducir el concepto de análisis de riesgo a la organización y utilizar una abstracción de la metodología de matrices de riesgo para hacer un primer análisis del contexto de seguridad de la organización, el cual será utilizado para seleccionar escenarios de seguridad y así elaborar procedimientos pertinentes al caso en la segunda actividad.

### _Datos de entrada

- Niveles de consecuencias desarrollados en la actividad de Mapeo y clasificación de información en la sección 01.

### _Productos

#### _Directos

- Listado de amenazas posibles a la organización priorizado por impacto posible y probabilidad de ocurrencia estimada por el equipo.

#### _Indirectos

- Mejor entendimiento de los posibles escenarios adversos por los que puede atravesar la organización.
- Mejores criterios de categorización colectiva de amenazas posibles.
- Mejores criterios de priorización de amenazas potenciales para su atención y establecimiento de controles de seguridad..

### _Preparación previa

En caso de realizar la actividad en digital, se sugiere disponer de una hoja de cálculo u otro software con todos los campos y formatos necesarios.

### _Materiales

En caso de realizar la actividad en físico:

- Notas adhesivas y marcadores o
- Piezas grandes de papel para pegar en la pared y marcadores

En caso de realizar la actividad en digital:

- Computadora
- Proyector
- Hoja de cálculo u otro software con los campos y formatos necesarios.

## _Instrucciones

**1.** Introducir al grupo el concepto de amenaza (Posible evento negativo ocurrido a un recurso determinado), considerando los siguientes aspectos:

- Estas pueden tener causas humanas y no humanas (desastres naturales, reacciones espontáneas, desgaste y mal funciones no programadas, etc.) Estas pueden ser intencionales o accidentales.
- Estas pueden ser provocadas o fortuitas.
- Estas pueden afectar a recursos físicos, digitales, humanos, legales y administrativos entre otros. De hecho muchas organizaciones consideran la afectación de su imagen y posicionamiento como un recurso, siendo una consideración válida dentro del ejercicio.

Por lo general, es más fácil para los participantes usar una estructura en la redacción de amenazas similares a estas:

> [Algo malo pasa]

A. Ausencia del director.
B. Ladrones entran a la oficina.

Que [algo malo le pase a algún recurso o actor vinculado a la organización].

A. Que hackeen la cuenta de Twitter.
B. Que se pierda el acceso a las cuentas bancarias.

Sin embargo, en algunas ocasiones esta forma de construir las amenazas puede resultar tan vaga que no representan posibles eventos sino otras cosas, como por ejemplo vulnerabilidades o ausencia de medidas de seguridad. En ese sentido se recomienda a los facilitadores asegurarse de que la redacción de las amenazas a lo largo del ejercicio corresponda a eventos. Si el facilitador lo considera conveniente, puede plantear una estructura de redacción que ayude a disminuir errores, por ejemplo:

Que [un actor] [ejecute una acción] a/sobre [un recurso] [provocando ciertas consecuencias – opcional]

A. Que un hacker introduzca un malware en la computadora del director de la organización.
B. Que el organismo de Inteligencia de mi país monitoree las llamadas telefónicas con las fuentes periodísticas exponiendo la integridad física de estas.



Que [un evento] [ejerza una acción] a/sobre [un recurso] [provocando ciertas consecuencias – opcional]

A. Que ocurra un terremoto de 7.5 o más, destruyendo el datacenter de la empresa donde se aloja la página web..
B. Que un apagón deje sin electricidad a la oficina imposibilitando el trabajo en las computadoras.

Esta redacción puede adaptarse para considerar amenazas sin adversarios o eventos claros, así como cualquier otra variación de las amenazas que no cubren directamente estas propuestas de redacción.

**2.** Pedir a los participantes que piensen en amenazas para la organización, tomar nota de estas y colocarlas de forma visible para todos.


Grafico 18. Mapeo de amenazas.

3. Con todas las amenazas en un mismo sitio, utilizar los niveles de impacto desarrollados en la actividad de Mapeo y clasificación de información y colocarlos como el eje vertical de una matriz, luego con la ayuda de los participantes asignar a cada amenaza un nivel de impacto ubicando la nota adhesiva o equivalente a la altura del nivel de impacto seleccionado.

- Se sugiere además de colocar los niveles de impacto cualitativos definidos anteriormente, disponer de una escala numérica como se muestra en el gráfico. Esto puede ayudar a cuantificar el nivel de riesgo luego de completar la actividad.

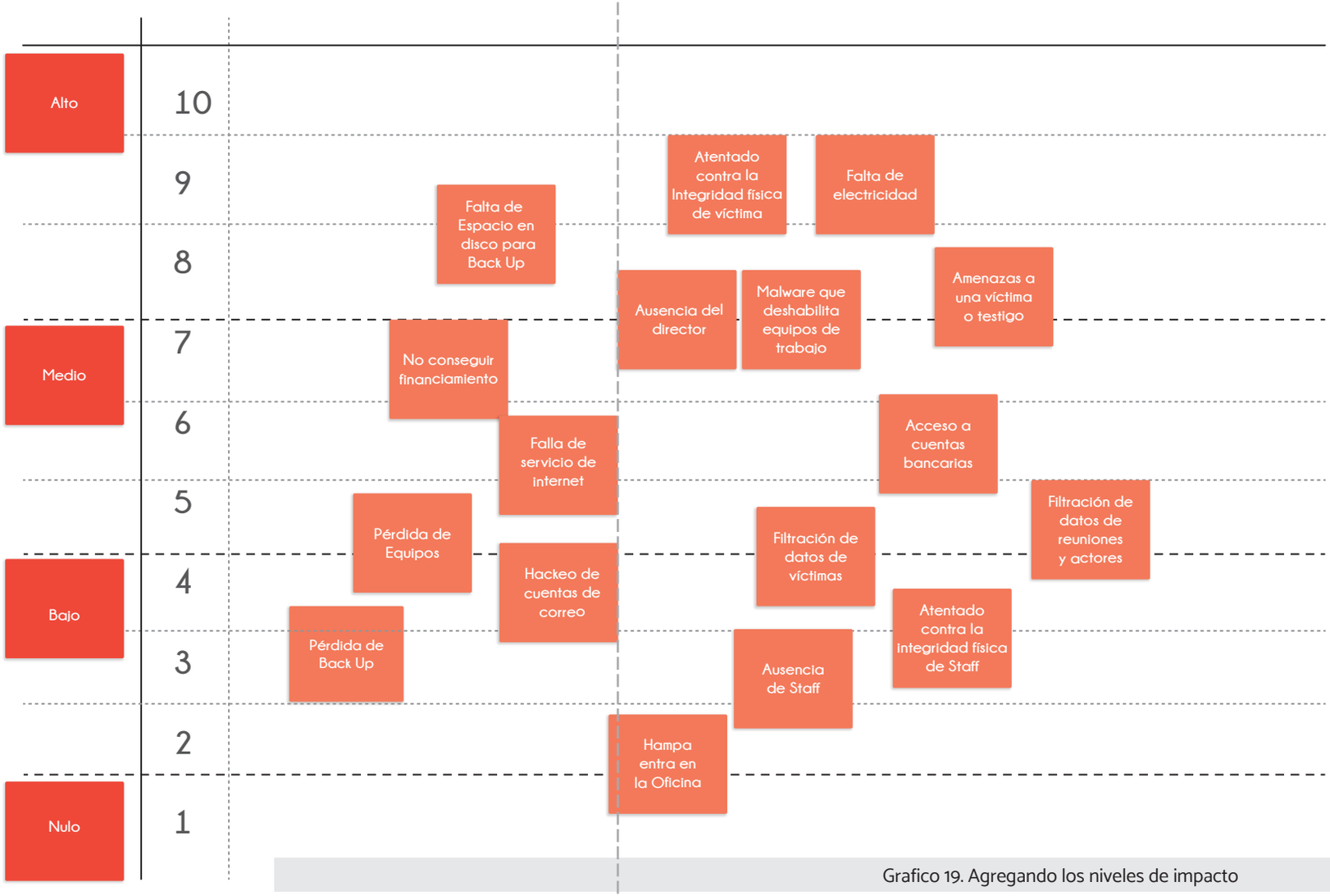



Grafico 19. Agregando los niveles de impacto

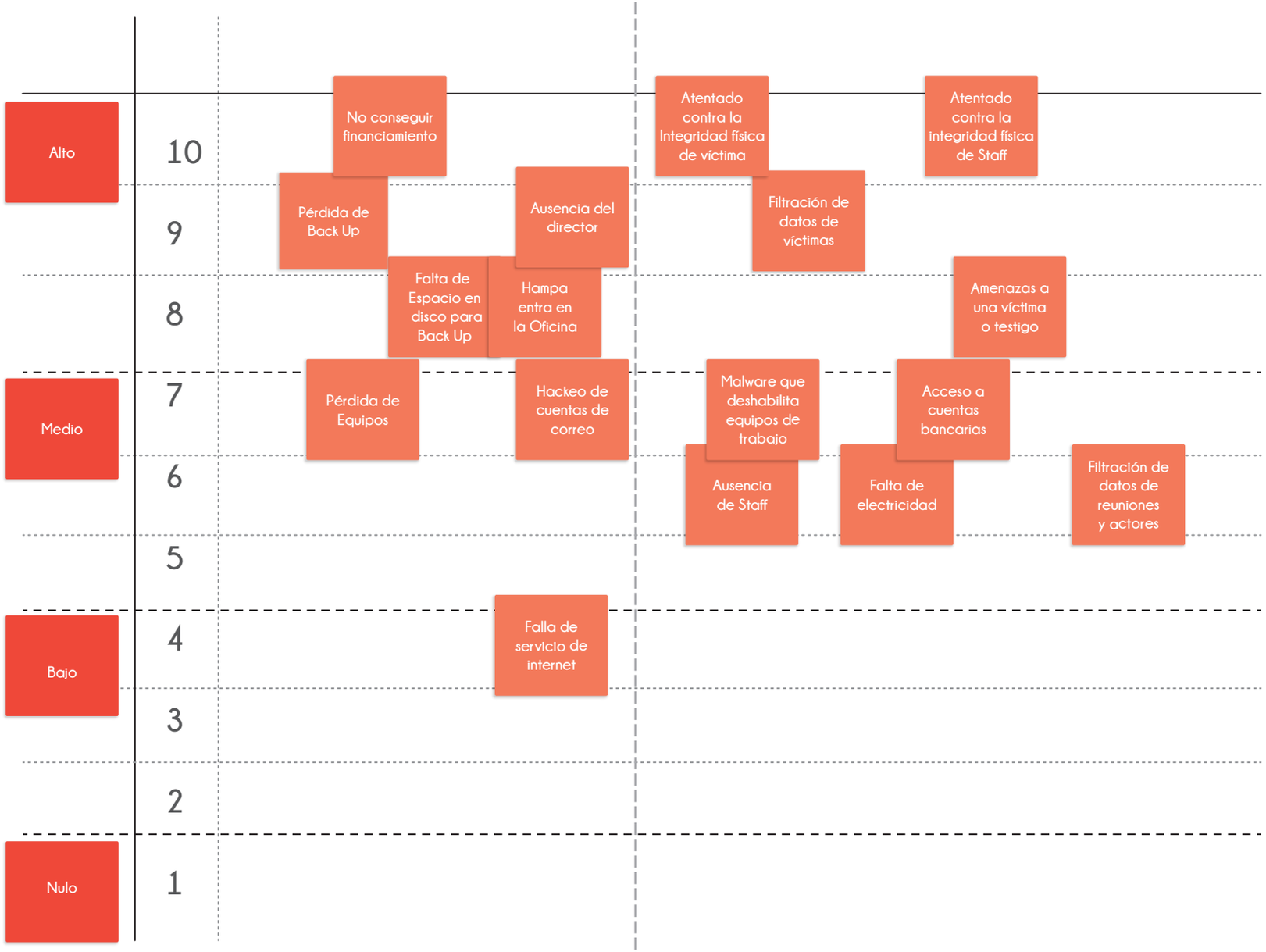



Grafico 20. Reorganizando las amenazas post niveles de impacto

**4.** Plantear el concepto de probabilidad de ocurrencia y definir una escala para representarla en la matriz de riesgo elaborada. Reorganizar en el eje horizontal con la ayuda del grupo las amenazas de tal modo que coincidan no solo con la escala de impacto sino también con la probabilidad de ocurrencia seleccionada en cada caso, completando la matriz de riesgo de la organización, como se muestra en el gráfico.

- En los gráficos se sugiere una escala del 1 al 10, esta puede ser cambiada por otro tipo de escalas como por ejemplo las descritas abajo. Sin embargo, si se quiere hacer un análisis numérico de las amenazas es necesario que la escala también sea numérica e igual a la escala utilizada para los niveles de riesgo,

  - Probabilidad baja, media y alta.
  - Probabilidad nula, baja, alta y certeza de ocurrencia.
  - Escala del 1 al 5.

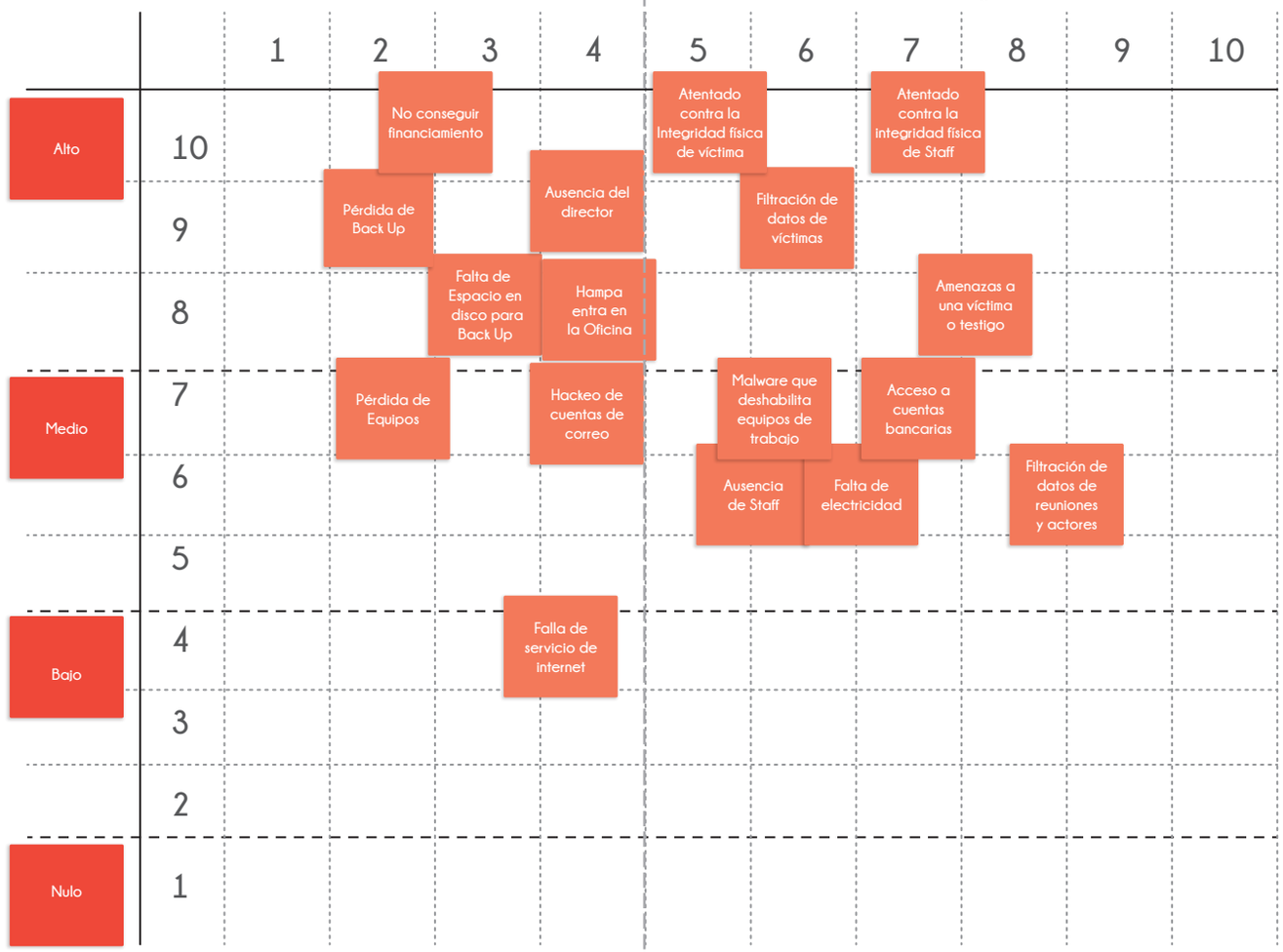



Grafico 21. Agregando los niveles de probabilidad de ocurrencia

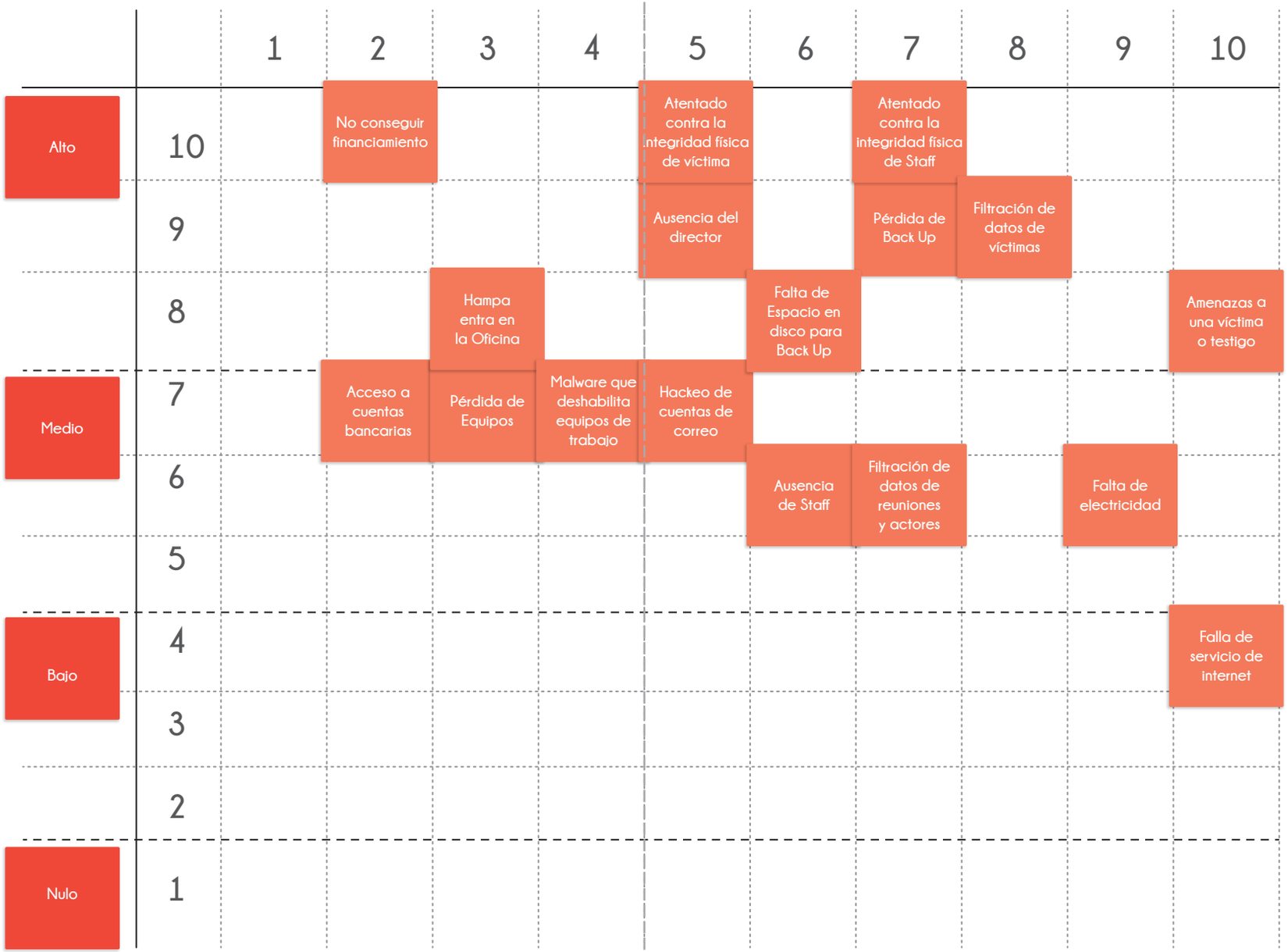





Grafico 22. Reorganizando las amenazas post niveles de probabilidad de ocurrencia.

**5,** Discutir sobre niveles de riesgo presentes en la matriz y realizar una lectura del contexto de seguridad de la organización a través de esta herramienta.

- Es esencial que los participantes tengan claro que las amenazas más importantes para atender deben ser aquellas que tienen altos niveles de impacto y altas probabilidades de ocurrencia asociados (en este caso aquellas más cercanas a la esquina superior derecha de la matriz).

- En el caso de querer hacer un análisis cuantitativo de los niveles de riesgo habiendo usado escalas numéricas en los niveles de impacto y probabilidad de ocurrencia, bastará con multiplicar estos valores para cada amenaza y ordenar de mayor a menor los resultados obtenidos (niveles de riesgo).

- Este ejercicio tiene como resultado un análisis subjetivo por parte de los miembros de la organización, por ningún motivo representa un análisis riguroso y preciso del contexto de riesgo de la organización. Incluso si el mismo equipo repitiera la actividad al día siguiente pudiera resultar una matriz de riesgo diferente.

- Esta matriz de riesgo, así como cualquier otro insumo que represente el contexto de riesgo de la organización, es un insumo temporal que no considera que los riesgos cambian a través del tiempo. Es muy importante hacer énfasis con los participantes que esta matriz representa "una foto" del estado de riesgo para ese momento en particular, y que la invitación es a repetir este ejercicio periódicamente para actualizar esta representación obtenida.

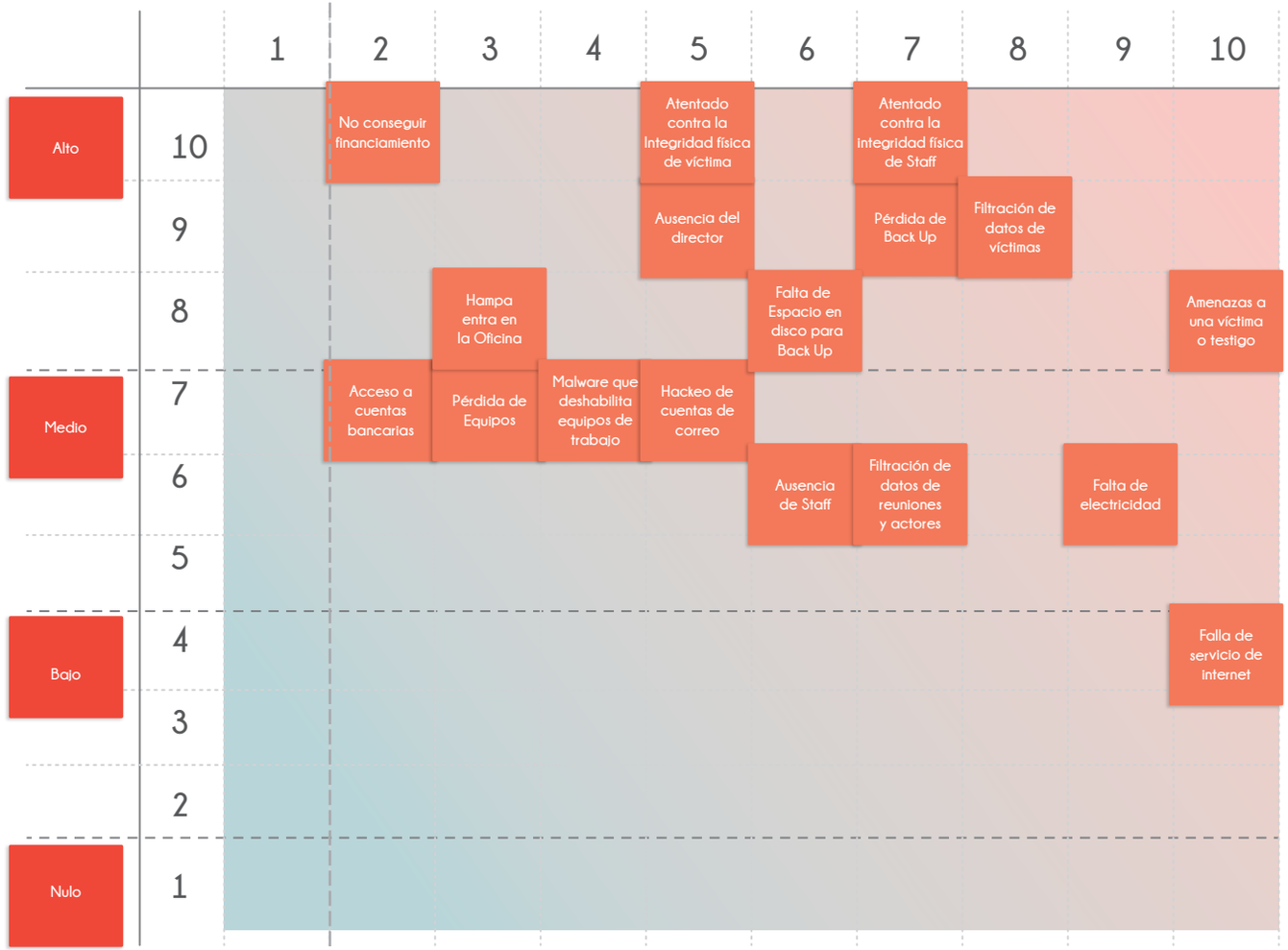



Grafico 19. Análisis de matriz de riesgo

## _Cierre de la actividad

Al finalizar la actividad se puede discutir y hacer énfasis en lo que se logró:

- Se definieron criterios para la detección de amenazas, y se hizo un mapeo contenido de las amenazas actuales propuestas por el equipo.
- Se desarrollaron criterios de estudio y priorización de las amenazas. También se emplearon estos criterios durante el ejercicio de amenazas mapeadas.
- Se introdujo una metodología de construcción de matrices de riesgo que puede ser replicada en el futuro por la organización.

## _Referencias


R20 SAFETAG

R21 Saferjourno




# 02_Introducción a los procedimientos de seguridad

Tiempo estimado: 60 min

## _Justificación

La idea de esta actividad es complementar las políticas desarrolladas anteriormente como estrategias preventivas con el desarrollo de procedimientos a ser aplicados durante incidentes de seguridad como estrategias reactivas que buscan mitigar el impacto de las amenazas una vez concretadas. Específicamente esta actividad busca abstraer los conceptos de elaboración de procedimientos, planes de comunicaciones, planes de sucesión y actividades de preparación en una sola dinámica que sirva de introducción al área de respuesta a incidentes desarrollada en la literatura de seguridad de la información.

## _Datos de entrada

- Matriz de riesgo.

## _Productos

### _Directos

- Procedimiento de seguridad inicial para uno o dos escenarios puntuales seleccionados.

### _Indirectos

- Herramientas para desarrollar cualquier otro procedimiento de seguridad faltante por parte de la organización.
- Mejor entendimiento de la importancia de las comunicaciones internas, externas y de la sucesión de responsabilidades durante la atención de incidentes de seguridad.

## _Preparación previa

En caso de realizar la actividad en digital, se sugiere disponer de una hoja de cálculo u otro software con todos los campos y formatos necesarios.

## _Materiales

- Pliegos de papel grandes para pegar en la pared.
- Notas adhesivas (preferiblemente de varios colores).
- Marcadores para escribir en las notas adhesivas.

## _Instrucciones

**1.** Revisar la matriz de riesgo levantada en la actividad anterior y seleccionar una o dos amenazas que se consideren pertinentes para levantar procedimientos de seguridad. Algunas consideraciones pueden ser:

- Es normal que hayan amenazas que dependan altamente de personal o aliados externos para su resolución, aunque es deseable que sean amenazas resolubles en mayor medida por los mismos integrantes de la organización, el primer tipo de amenaza es válido para desarrollar la actividad.

**2.** Para cada amenaza, que desde ahora serán tratadas como incidentes de seguridad ya que se estará preparando el procedimiento para su ocurrencia, hacer una lluvia de idea de acciones que se deberían tomar como pasos, anotar cada uno en notas adhesivas y pegar en el papel o pared, luego reordenar a medida que se agregan nuevos pasos. Como ayuda para el grupo, usualmente las acciones que se toman en un procedimiento buscan:

- Minimizar el daño.
- Limpiar artefactos restantes del incidente.
- Reanudar actividades tan pronto como se pueda.


Grafico 20. Pasos del procedimiento



**3.** Para cada paso preguntar quién lo ejecutaría. Anotar en una nota adhesiva y colocar en una segunda columna en la pared junto al paso en cuestión, se puede preguntar al grupo quien supliría a este responsable en el caso de que no se encuentre durante el incidente. En los casos en que aplique tomar nota y colocar estos suplentes debajo del responsable principal como muestra el grafico.

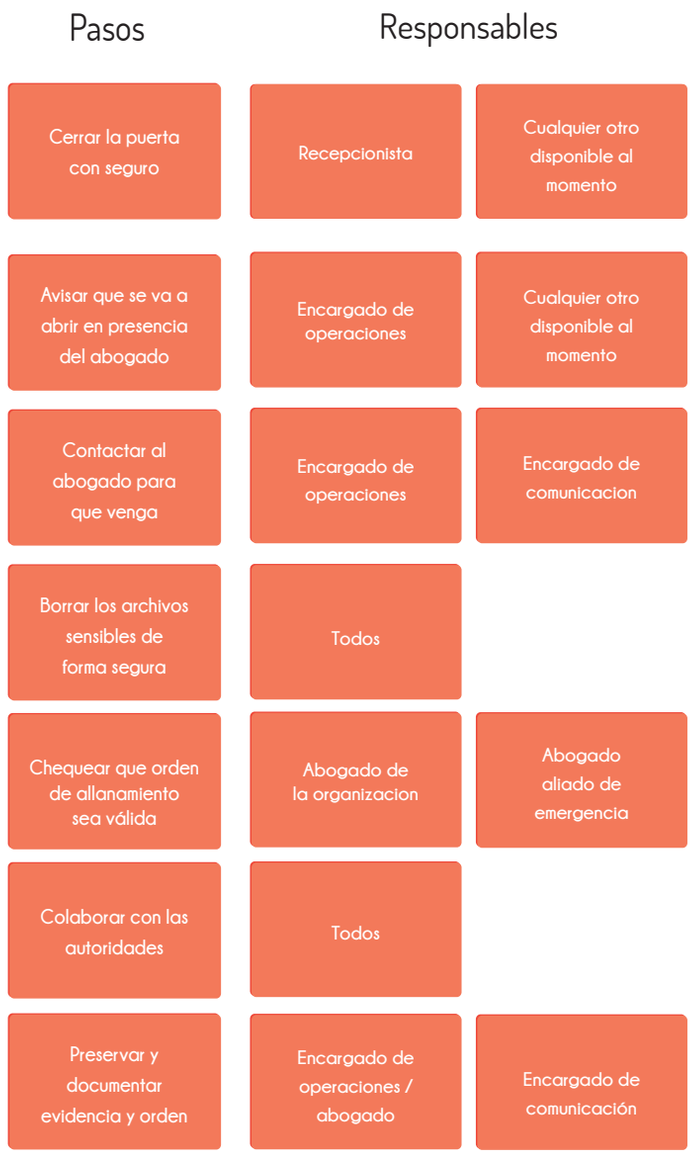



Grafico 21. Responsables por paso

**4.** Con consenso en el grupo sobre los pasos del procedimiento, preguntar en qué puntos se deben establecer comunicaciones con actores externos a la organización. La idea es anotar estos puntos de comunicación como nuevos pasos (idealmente en un color diferente) e integrarlos a los pasos del procedimiento reordenando los pasos existentes.

- Estas comunicaciones normalmente son obligatorias o altamente deseables para resolver el incidente, como redes de aliados, proveedores externos, etc.
- Es posible que en la misma dinámica de la actividad se haya adelantado este mapeo de comunicaciones en el paso 2 de forma natural, en ese caso con completar cualquier comunicación faltante y continuar será suficiente.
- Para cada paso relacionado a comunicaciones externas, verificar que siempre aparezca a quién se contacta, ya sea en el paso o en el responsable.


Grafico 22. Pasos del plan de comunicación

**5.** Crear una tercera columna con el encabezado "Preparación" y para cada paso preguntarle al equipo ¿Qué hace falta garantizar ANTES de que ocurra el incidente para que se pueda cumplir este paso?. Tomar nota de cada paso de preparación en una nota adhesiva y colocarla junto al paso correspondiente, es normal que algunos pasos no tengan acciones de preparación asociadas.

Algunos ejemplos usuales de pasos de preparación son:

- que A tenga el contacto de B consultor externo.
- que C sepa como apagar el servidor interno.
- que todos sepan borrar información de forma segura.

| Pasos | Responsables | | Preparación |
|---|---|---|---|
| Cerrar la puerta con seguro | Recepcionista | Cualquier otro Disponible al momento | |
| Avisar que se va a Abrir en presencia Del Abogado | Encargado de operaciones | Cualquier otro Disponible al momento | Poner a disposición Texto con respaldo Legal para el cierre |
| Contactar al Abogado para que venga | Encargado de operaciones | Encargado de Comunicaciones | Proveer a encarg. de comunic. y operaciones con # del Abogado |
| Borrar los archivos sensibles de forma segura | Todos | | Entrenamiento al Equipo sobre Borrado seguro |
| Alertar a orgs aliadas | Director | Encargado de Comunicaciones | Definir y Comunicar A orgs aliadas Canal de comunic. |
| Alertar a organizaciones Aliadas | Abogado de la organización | Abogado Aliado de emergencia | |
| Colaborar con las autoridades | Todos | | |
| Preservar y Documentar Evidencia y Orden | Encargado de operaciones / abogado | Encargado de Comunicaciones | Encargado de operaciones / abogado |

Grafico 23. Preparación previa para el procedimiento

**6.** Discutir con el grupo ¿Cómo se comunicarían entre ellos durante la resolución del incidente? y guiar la discusión sobre qué canales se consideran seguros y confiables para mantener al grupo comunicado durante el incidente, así como cuáles se utilizarían de manera formal durante éste tipo de incidente. Se sugiere tomar nota de estos canales y listarlos en orden de prioridad en caso de que el primero falle durante el incidente.

Vale la pena recordar que diferentes incidentes pueden afectar diferentes vías de comunicación.

**7.** Sugerir al equipo vaciar la información que se recopiló durante la actividad en un documento formal. Se puede utilizar la plantilla 4 disponible en el sitio web de este material (https://sda.guerracarlos.org).


Grafico 24. Orden de comunicaciones internas



## _Cierre de la actividad

Al finalizar la actividad se puede discutir y hacer énfasis en lo que se logró:

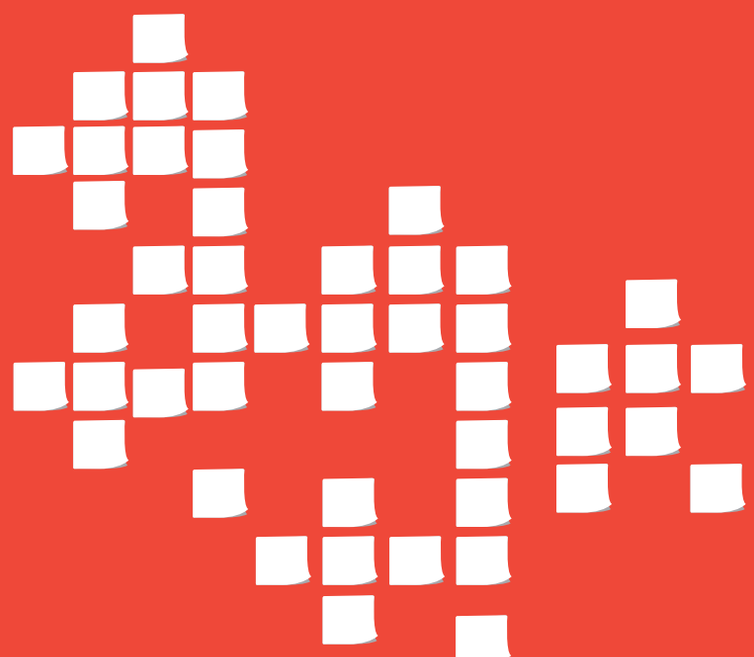
- Se elaboraron procedimientos reales para incidentes específicos.
- Se asociaron los pasos del procedimiento con encargados y sucesores en caso de no estar disponibles.
- Se integró un plan de comunicaciones externas al procedimiento.
- Se establecieron las bases de comunicaciones internas durante incidentes.
- Se exploraron los pasos para construir procedimientos de seguridad con la metodología utilizada.

Luego de finalizada la actividad, vale la pena proponer al grupo después de sucedido cualquier incidente, realizar una reunión posterior en donde el equipo se haga al menos las siguientes preguntas:

- ¿Qué pasó y en qué momentos?
- ¿Qué tan bien respondió el equipo al incidente?
- ¿Se siguieron los procedimientos? ¿Éstos fueron adecuados?
- ¿Hubo pasos o acciones tomadas que inhibieran la recuperación del incidente?
- ¿Qué haría el equipo diferente si pasa algo similar en el futuro? ¿Qué acciones correctivas pueden prevenir incidentes similares en el futuro?
- ¿Qué indicadores hay que revisar en el futuro para detectar incidentes similares?
- ¿Qué herramientas o recursos se necesitan para analizar, detectar y mitigar futuros incidentes?.

## _Referencias

R22 Umbrella: security made easy - Android App I Security First
R23 Digital First Aid Kit - Kit de primeros auxilios digitales
R24 AccessNow Digital Security Helpline - Línea de ayuda en seguridad digital



# 04_ Cierre

# 01_ Conclusión

Después de ejecutar las actividades propuestas en este manual habremos dotado a la organización de criterios y herramientas para comenzar un plan de seguridad coherente y robusto. Es importante resaltar que las políticas y procedimientos desarrollados en este manual representan un primer acercamiento a la elaboración de un plan de seguridad formal y en la medida en que la organización se sienta cómoda, se debería profundizar y complementar con otros aspectos y estrategias que cubran los espacios faltantes en la metodología propuesta.

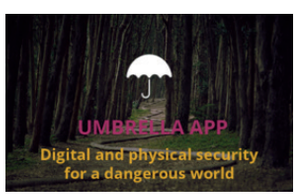
Además de desarrollar políticas escritas de seguridad organizacional, se recomienda consultar referencias sobre seguridad de la información e integral para complementar el desarrollo de políticas y procedimientos con la generación de un plan de capacitación en seguridad para todo el equipo de la organización. Este proceso de capacitación puede ayudar a mantener de una forma más efectiva las políticas y procedimientos desarrollados así como una integración efectiva de principios de seguridad en los procesos diarios de la organización.

A continuación se mencionan algunos proyectos de interés para los facilitadores en seguridad para las organizaciones, que además de servir de inspiración e insumo para este manual, son referencias complementarias para ampliar el alcance del trabajo en seguridad que puede llevar a cabo una organización que hace activismo o cualquier otra forma de incidencia en el área de Derechos Humanos:

# 02_ Referencias

Holistic Security | Tactical Technology Collective
Manual que aborda actividades para explorar el estado de la seguridad de la organización desde un punto de vista integral (digital, físico y emocional), así como actividades de colaboración para generar estrategias contra los riesgos detectados más relevantes. Utiliza una narrativa de construcción de conocimiento a través de la facilitación.
https://holistic-security.tacticaltech.org

SAFETAG | Internews
Metodología completa para la evaluación y proposición de hojas de ruta para la resolución de vulnerabilidades y enfrentamiento de amenazas para organizaciones que realizan activismo
https://safetag.org




Umbrella
Aplicación Android con material de capacitación en estrategias ante riesgos de seguridad físicos, digitales y emocionales, contiene listas de chequeo propuestas ante situaciones puntuales.
https://secfirst.org


Digital First Aid Kit | Digital Defenders Partnership
Conjunto de guías de respuesta rápida ante incidentes de seguridad frecuentes.
https://rarenet.github.io/DFAK/es/



Security Education Companion | Electronic Frontier Foundation
Conjunto de recursos para facilitadores en temas de seguridad digital y privacidad.
https://sec.eff.org

Surveillance Self-Defense | Electronic Frontier Foundation
Conjunto de guías rápidas sobre temas de seguridad digital y análisis de riesgo para personas haciendo activismo.
https://ssd.eff.org


Security in a box | Tactical Technology Collective - FrontLine Defenders
Conjunto de guías de capacitación en temas de seguridad de la información dirigido a activistas de Derechos Humanos, resulta útil para ejecutar planes de capacitación y revisar directivas y consideraciones de seguridad para políticas.
https://securityinabox.org/en/


Me and my shadow - Training curriculum | Tactical Technology Collective
Herramienta de construcción de programas de capacitación en seguridad digital con conceptos y actividades asociadas.
https://myshadow.org/train