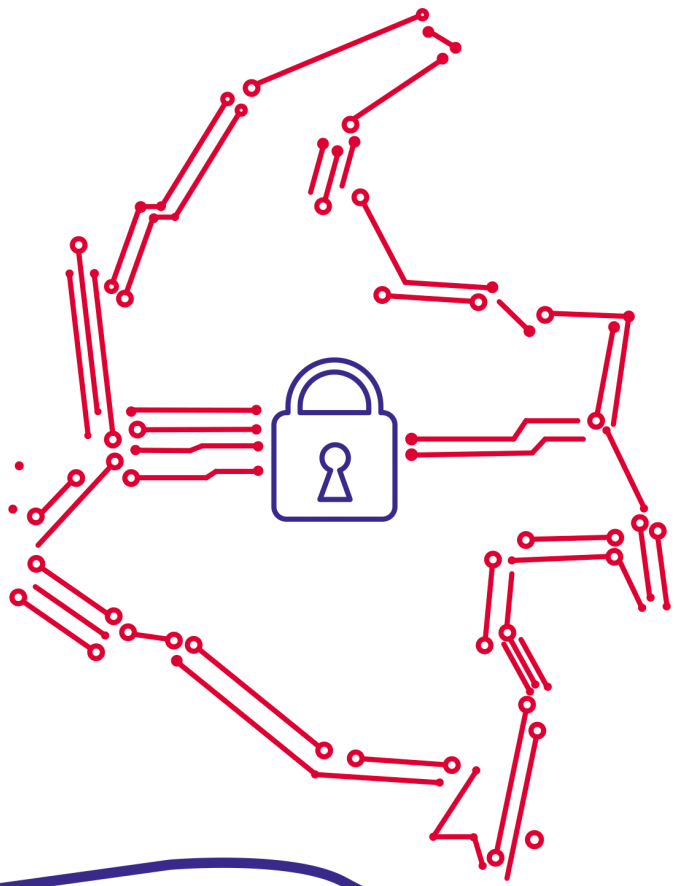
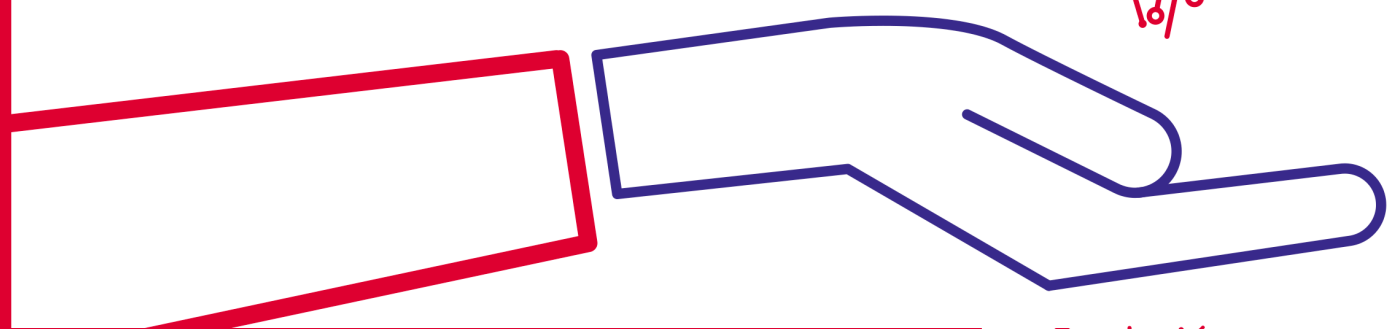
# Currículo para personas auditoras de seguridad digital

## Una propuesta de ajuste a la metodologia **SAFETAG** en Colombia

**Autores**
Pilar Sáenz
Santiago Hernández
Lucía Camacho

**Colaboradores**
Brian Venera
Cristian Torres
Andrés Restrepo
Stéphane Labarthe
Christian Peñaranda





Fundación Karisma

Fundación
Karisma

Bogotá, Colombia
2018

En un esfuerzo para que todas las personas tengan acceso al conocimiento, Fundación Karisma está trabajando para que sus documentos sean accesibles, eso quiere decir que su formato incluye metadatos y otros elementos que lo hacen compatible con herramientas como lectores de pantallas o pantalla braille. El propósito del diseño accesible es que todas las personas puedan leer, incluidas aquellas que tienen algún tipo de discapacidad visual o de dificultad para la lectura y comprensión.

Más información sobre documentos accesibles en: http://www.documentoaccesible.com/#que-es

Consulta este documento en línea en el sitio web Karisma en: https://karisma.org.co/descargar/curriculo-para-auditores-de-seguridad-digital/

**Autores:**
Pilar Sáenz
Santiago Hernández
Lucía Camacho

**Colaboradores:**
Brian Venera
Cristian Torres
Andrés Restrepo
Stéphane Labarthe

**Diagramación:**
Rubén Urriago

# Tabla de Contenido

# 1. SAFETAG PARA COLOMBIA

Realizar labores sociales en Colombia en este momento implica, en cierto modo exponer de manera significativa la integridad personal y la vida.

Colombia actualmente se encuentra en un periodo de posconflicto. Las Fuerzas Armadas Revolucionarias de Colombia (FARC), el grupo armado más antiguo y más organizado del conflicto interno, firmó un acuerdo de paz con el gobierno nacional en el año 2016. Con el fin del conflicto, el grupo armado hizo entrega de sus armas y sus integrantes se movilizaron a zonas de concentración. En las zonas donde había mayor presencia de las FARC es donde en general había menor presencia estatal lo cual generó unos vacíos de poder en estas zonas, tras la retirada del grupo armado.

Como resultado del retiro de estos grupos armados y la ausencia del Estado en las zonas en las que estos tenían presencia, se ha incrementado la cantidad de grupos al margen de la ley que aprovechan el vacío de poder para ejercer de forma violenta el control del territorio ya sea porque existen conflictos de tierras, por que hay presencia de cultivos o laboratorios asociados al narcotráfico o presencia de otros grupos al margen de la ley. En estos territorios las voces de personas defensoras de derechos humanos, líderes y lideresas sociales, periodistas y activistas de la región son las que han expuesto estas problemáticas y son, en consecuencia, quienes han sufrido los mayores ataques. Desde la firma del acuerdo de paz, el asesinato de líderes y lideresas sociales se ha incrementado en una forma que no tiene precedente.

Según la Defensoría del Pueblo de Colombia se han asesinado 343 líderes y lideresas sociales desde el 01 de enero de 2016 hasta el 22 de agosto de 2018. Mientras tanto, el gobierno nacional emite comunicados desmintiendo las cifras de la Defensoría del Pueblo y de la ONU.[1]

En los últimos meses además hemos constatado que las amenazas que se ejercen sobre líderes y lideresas arriban a través de correos electrónicos, mensajes de WhatsApp y redes sociales. Ante este panorama, es de vital importancia diseñar e implementar métodos para reducir los riesgos de las organizaciones sociales en el desempeño de sus labores, tanto en el ámbito digital como en el personal. Muchas de las actividades que realizamos en línea nos pueden exponer de forma personal y organizacional.

1 Para ver los comentarios del Relator Especial sobre la situación de los defensores de los Derechos Humanos de Naciones Unidas en su última visita a Colombia, se puede consultar: https://colombia2020.elespectador.com/politica/las-cifras-de-la-fiscalia-noconvencen-relator-de-la-onu

En este contexto realizar auditorías de seguridad digital a organizaciones de la sociedad civil en Colombia puede contribuir a mejorar su preparación ante las diferentes amenazas a las cuales se ven expuestas. Sin embargo, es necesario desarrollar una capacidad nueva entre los expertos en seguridad digital para trabajar con las organizaciones de la sociedad civil, que pasa no solo por comprender la metodología de SAFETAG, sino también el contexto de las organizaciones con las cuales se trabajará, comprender sus necesidades y capacidades y la forma como se pueden construir relaciones de confianza que faciliten la realización de estos ejercicios.

Dentro de este documento se encuentra plasmado el aprendizaje producto de nueve auditorías con organizaciones de sociedad civil (en adelante OSC), dos de estas utilizando un ajuste de la metodología de SAFETAG, el entrenamiento de un grupo de personas auditoras, la preparación de los materiales de entrenamiento, el ajuste de la metodología SAFETAG de acuerdo a la realidad nacional, el desarrollo de una metodología de riesgos, una herramienta de manejo de riesgos, la estructura del documento de auditoría y el currículo para el entrenamiento de personas auditoras.

Fue un arduo trabajo dentro del cual compartimos nuestra experiencia a la vez que aprendimos de las prácticas y conocimientos de quienes realizan auditorías en escenarios tradicionales de empresas y organismos del Estado. En el proceso con las organizaciones aprendimos también cuán importante es construir confianza, espacios flexibles de aprendizaje mutuo y sobre todo comprender y ajustarnos a sus limitaciones, no sólo en términos de capacidad o conocimiento sobre el tema sino también sobre el tiempo. Aprendimos que el tiempo para las organizaciones es uno de sus recursos más limitados y que al menos inicialmente era imposible realizar un ejercicio que tarde más de dos días. Aunque SAFETAG no plantea la realización de capacitaciones, nosotros entendimos que para causar un impacto permanente, dictar un taller de seguridad digital para estas organizaciones era indispensable.

Por esta razón decidimos dedicar la mitad del tiempo que nos brindaban las organizaciones en esta labor. Esto nos ayudó de manera significativa en el establecimiento de una relación de confianza con los integrantes de las organizaciones y a crear un entendimiento frente a la actividad de la auditoría. Las capacidades creadas en los integrantes de las organizaciones durante el taller y la confianza generada permitió que las entrevistas de auditoría se ejecutaran sin fricción. Que compartieran sus experiencias, buenas y malas, sus temores y se sinceraran en el ejercicio.

En ambos casos se logró conocer las actividades principales de los procesos críticos de la organización y sus falencias técnicas sin tener que realizar ejercicios invasivos sobre su infraestructura. Esto nos permitió también que las entrevistas fueran aprovechadas para el mejor reconocimiento entre las partes.

De parte de los y las auditoras, durante el taller inicial y en nuestras charlas de retroalimentación luego de las entrevistas de auditoría e incluso en el taller de cierre, logramos

generar una sensibilidad mayor frente a la importancia del trabajo que hacen las organizaciones de sociedad civil. A la vez, que el intercambio entre ellos y las organizaciones también les abrió los ojos a una realidad desconocida, la que enfrentan diariamente estas organizaciones y sus miembros. Así, entre los aprendizajes adquiridos por parte de las personas auditoras no solo se incluyen conocimientos técnicos puntuales sobre seguridad digital y tecnología; sino también una mejor comprensión del contexto del país, y de las amenazas a las que particularmente están expuestas las OSC. Por parte de las OSC auditadas, se fortalecieron conocimientos sobre el trabajo social en Colombia y cómo sus labores interactúan con riesgos y vulnerabilidades en seguridad digital que pueden con el mejoramiento de ciertos hábitos, reducir o prever.

SAFETAG, como proyecto, también propone un currículo para la formación de nuevos y nuevas auditoras, que desde Karisma ajustamos al contexto nacional. Este ejercicio nuevo nos llevó a la realización de dos talleres y una serie de actividades de preparación para las auditorías con personas expertas en seguridad digital en proceso de formación como personas auditoras para organizaciones de sociedad civil.

Este currículo es el resultado de ese ejercicio, sintetiza el proceso de formación que llevamos a cabo con un grupo de 9 personas expertas en seguridad digital que no solo estuvieron en las actividades sino que alimentaron este texto. Reconocemos su compromiso y dedicación para con el proyecto y agradecemos los aportes que hicieron para la realización de este currículo.

# 2. INTRODUCCIÓN A SAFETAG

## 2.1. ¿Qué es?

SAFETAG es un marco de referencia y lista de chequeo creada de forma abierta bajo el ala de Internews. Fue desarrollado con la finalidad de poder adaptar las técnicas tradicionales de pruebas de hacking ético, auditorías de seguridad de la información y metodologías de riesgos a organizaciones civiles sin ánimo de lucro y a poblaciones vulnerables, con la finalidad de poder ayudarlas a mejorar su estado de seguridad teniendo en cuenta la limitación de sus recursos, tanto técnicos como financieros.

El marco de referencia fue desarrollado con base en estándares establecidos para la realización de auditorías de seguridad y las mejores prácticas para organizaciones de sociedad civil. El objetivo es que las personas auditoras puedan apoyar a la organización y sus colaboradores en la creación de una cultura de seguridad mediante un plan de trabajo que considere etapas como la identificación, análisis y gestión de riesgos y vulnerabilidades de seguridad identificadas, con el fin de lograr alcanzar una madurez suficiente en seguridad digital que permita a la organización tratar los riesgos asociados al manejo de información.

La realización de auditorías de seguridad digital para organizaciones de sociedad civil es una necesidad mundial, sin embargo es preciso que este marco de referencia se adapte a las particularidades del contexto y enfoque de cada organización para responder de mejor manera a las amenazas puntuales que pueden estar enfrentando las organizaciones en un lugar específico y según sus actividades.

De la misma manera que la metodología puede ser ajustada, también es necesario desarrollar una sensibilidad especial entre la comunidad técnica que realizará las auditorías. No se trata solamente de aportar una serie de conocimientos, metodologías y técnicas sino de introducir las singularidades del mundo de las organizaciones de sociedad civil, las amenazas a las cuales están expuestas, las capacidades que tienen y las que necesitan desarrollar, el tipo de recursos a los que pueden acceder y en particular el contexto en el cual se encuentran.

## 2.2. Una metodología adaptada

La metodología de SAFETAG fue adaptada por la Fundación Karisma considerando el contexto de las organizaciones de la sociedad civil en Colombia. Se decidió trabajar con organizaciones legalmente constituidas, de carácter mediano, que no estuvieran bajo

amenaza directa, que ya hubieran sufrido algún incidente de seguridad digital, con las que se podía construir una relación de confianza que permitiera el desarrollo de la metodología.

El objetivo principal de las actividades realizadas con las organizaciones no solo es el de ejecutar pruebas técnicas y recomendar herramientas específicas, sino la creación de conciencia de los riesgos a los cuales se enfrentan las organizaciones, sus colaboradores y beneficiarios en el día a día de sus actividades, tanto por el uso de herramientas digitales e internet, como por sus comportamientos fuera de línea.

Teniendo en cuenta la escasa madurez en materia de seguridad digital dentro de las organizaciones de la sociedad civil con las que hemos decidido trabajar, la adaptación que hemos realizado de la metodología de SAFETAG hace que la orientación del ejercicio sea más hacia un proceso exploratorio y no hacia una auditoría tradicional. Si bien sabemos que el ejercicio es limitado, también creemos que se ajusta mejor a las capacidades que tienen las organizaciones para implementar medidas de acuerdo a sus capacidades. Un ejercicio a profundidad podría producir efectos indeseados, incluyendo la pérdida de confianza, sentimiento de impotencia frente a la magnitud de los cambios necesarios para mejorar, y en general la generación de un sentimiento de desilusión frente a las posibilidades de mejora.

Por esta razón, priorizamos una mirada que se centra en entender el estado de la organización, sus capacidades y en dar elementos que permitan elevar su grado de entendimiento sobre la seguridad digital y los riesgos, de forma tal que al final del ejercicio se puedan establecer acciones de mejora acordes con los recursos de la organización.

Dentro de los principales ajustes al modelo propuesto por SAFETAG, Karisma ve la necesidad de introducir dos momentos previos a la auditoría que sirven como preparación, el primero es un cuestionario para establecer una línea base del estado de seguridad digital de la organización y el segundo es un taller de sensibilización, con la mayor parte de las personas que hacen parte de la organización, que permita de forma didáctica introducir el modelo de riesgo y dar algunas recomendaciones básicas generales para mejorar la seguridad digital en sus actividades cotidianas.

### 2.2.1. Etapas de auditoría basada en safetag

Ahora bien, en rasgos generales la auditoría se compone de las siguientes etapas:

0. Etapa cero:
    a. Evaluación del estado de la organización para establecer si cumple con los requerimientos para realizar la auditoría
    b. Contacto inicial con la organización
    c. Firma del memorando de entendimiento para la realización de la auditoría

1. Etapa preliminar:
   a. Envío del "Cuestionario de análisis de riesgo en seguridad digital" que incluye las siguientes partes: 15 preguntas generales, 18 sobre infraestructura y herramientas digitales, 14 sobre seguridad, y 7 sobre riesgos y amenazas
   b. Realización de un taller de sensibilización en seguridad digital dirigido a los directivos, integrantes y colaboradores de la organización de la sociedad civil
2. Etapa de auditoría
   a. Levantamiento del contexto organizacional
   b. Realización del OSINT (del inglés Open Source Intelligence), incluyendo información de uso de redes sociales
   c. Realización de entrevistas a directivos y funcionarios claves de la organización. Se indaga en particular sobre la forma de gestión de la información y el manejo de la infraestructura de tecnología
   d. Análisis de procesos y activos
   e. Análisis de vulnerabilidades
   f. Modelado de riesgos
   g. Identificación de adversarios y capacidades
   h. Identificación de amenazas
   i. Análisis de la seguridad física del sitio
   j. Análisis en línea de los dominios y de los sitios web de la organización
3. Etapa final: informe, cierre, recomendaciones
   a. Redacción del contexto organizacional
   b. Documentación del informe de auditoría
   c. Entrega del informe y reunión de cierre
   d. Establecimiento del seguimiento a los hallazgos

A futuro se espera establecer canales de comunicación, actividades donde se profundice en algunos de los temas que quiera abordar la organización o implementaciones de recomendaciones específicas. Sin embargo, este tipo de actividades están sujetas tanto a la capacidad de las personas que realicen las auditorías, los recursos a los que se tenga acceso y los tiempos que demanden.

### 2.2.2. Conceptos clave de la metodología safetag

Las auditorías de SAFETAG consisten en múltiples pasos de recolección y confirmación de información, así como de ejercicios de investigación que permiten crear capacidades en las organizaciones.

Aun cuando en el ejercicio de adaptación que Karisma hace de la metodología SAFETAG no se siguieron estrictamente todos los pasos, queremos referirnos al proceso en su totalidad y presentar el ciclo completo de la auditoría:

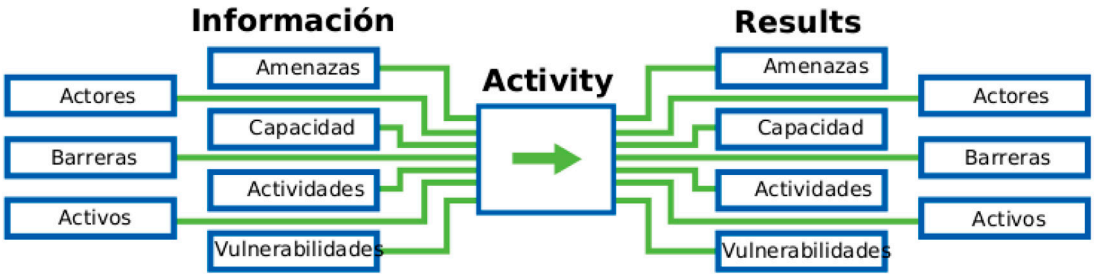

*Actividades de SAFETAG*

Fuente: "El sistema de auditorías y plantillas de evaluación para grupos de defensoría"[2]

Estamos de acuerdo con que el proceso de una auditoría es cíclico. Se identifican nuevas amenazas, vulnerabilidades, capacidades y barreras de impacto en las actividades existentes y a implementar en el futuro. Al mismo tiempo, el o la auditora a través de conversaciones, entrenamientos y actividades de grupo está capacitando a las organizaciones y abordando amenazas críticas o sensibles dentro de los plazos.

Este proceso iterativo finalmente lleva al auditor a un punto en el cual considera que se han identificado los puntos críticos y que ahora la organización está lista para seguir adelante por su cuenta a partir de las recomendaciones que se formulen. Cada objetivo requiere de cierta información básica, y entrega más información dentro de este proceso cíclico. Cada objetivo tiene un "mapa" de flujo de datos en el cual sus actividades están basadas en el siguiente gráfico:

2 SAFETAG (s.f.) "El sistema de auditorías y plantillas de evaluación para grupos de defensoría", pg. 6, disponible en https://github.com/SAFETAG/SAFETAG/releases/download/v0.4/SAFETAG.Overview.Espanol.pdf




*El Flujo De La Información de SAFETAG*

Fuente: "El sistema de auditorías y plantillas de evaluación para grupos de defensoría"[3]

3 SAFETAG (s.f.) "El sistema de auditorías y plantillas de evaluación para grupos de defensoría", pg. 7, disponible en https://github.com/SAFETAG/SAFETAG/releases/download/v0.4/SAFETAG.Overview.Espanol.pdf

# 3. PARTE CERO

## 3.1. CONSTRUCCIÓN DEL CONTEXTO DE PAÍS

### 3.1.1. Resumen

La construcción del contexto de país es una parte importante de la etapa preliminar, pues se reconoce a la organización como parte de una realidad nacional social y política determinada que de alguna manera influye en las labores que ésta última lleva a cabo y el riesgo que afronta por la realización de sus actividades misionales.

### 3.1.2. Por qué importa y por qué lo hacemos

El contexto de país alude especialmente a las condiciones de seguridad a nivel nacional que pueden impactar de manera directa o indirecta las labores de las organizaciones de la sociedad civil, y que convierten a sus miembros en posibles objetivos vulnerables o de amenaza. Este contexto incluye también una referencia al marco normativo y al estado de desarrollo de políticas públicas en materia de seguridad digital, seguridad nacional y vigilancia de las comunicaciones.

Es de especial relevancia el conocimiento sobre la adopción de tecnologías de vigilancia de las comunicaciones por parte de autoridades estatales y la falta de control en la utilización de dichas tecnologías que pueda poner en riesgo a las personas defensoras de derechos humanos, activistas, periodistas y en general a la comunidad y las organizaciones de sociedad civil. Finalmente, la ausencia o incapacidad del Estado por combatir los crímenes contra estas personas y la falta de garantías para el ejercicio de su trabajo, incluida la presencia de otros actores que generen amenazas directas contra ellos y ellas.

Es ideal que la redacción del contexto de país se efectúe bajo una contrastación de los mas recientes eventos de actualidad nacional a nivel político y social, el cual podrá ser documentado o apoyado con notas en prensa, informes de otras organizaciones y artículos de investigación recientes sobre el tema. Este contexto es preciso redactarlo de una manera descriptiva que en todo caso provea información sobre las condiciones que pueden afectar o afecten a organizaciones de la sociedad civil que lleven a cabo labores de defensa o protección de los derechos humanos.

### 3.1.3. Materiales requeridos

- Presentación
- Notas en prensa
- Informes de otras organizaciones y artículos de investigación

## 3.2. CONTEXTO SOBRE VIGILANCIA DE LAS COMUNICACIONES EN COLOMBIA

### 3.2.1. Resumen

Esta presentación tiene como propósito dar a conocer el contexto colombiano, en el que la vigilancia masiva de las comunicaciones tienen graves y todavía recientes antecedentes en el país.

La presentación aborda en su orden: los sistemas de vigilancia masiva que han sido utilizados en Colombia por parte del Estado, el catálogo de tecnologías de vigilancia y sus capacidades de intromisión o injerencia en la intimidad y comunicaciones de las personas, y una breve historia de las políticas públicas en ciberseguridad y seguridad digital que han sido formuladas en el país y cuál es el alcance de cada una; todo ello articulando casos y hechos reales que demuestran que las vulnerabilidades y riesgos son todavía actuales.

### 3.2.2. Por qué es importante

Revisar esta presentación resulta importante en la medida que aproxima una realidad a las personas auditoras que no necesariamente conocen el tipo de tecnologías que se emplean en el país ni el contexto regulatorio o simplemente desconocen las capacidades del Estado para vigilar a quienes llevan a cabo actividades de impacto social o trabajo con comunidades de base como líderes sociales, entre otros.

La presentación además ayuda a identificar adversarios que no son tenidos en cuenta al momento de analizar los riesgos digitales.

### 3.2.3. Materiales que se necesitan

- Presentación sobre vigilancia de las comunicaciones en Colombia (*Ver anexo 5*)

## 3.3. SELECCIÓN DE LA ORGANIZACIÓN A AUDITAR

### 3.3.1. Resumen

Para llevar a cabo la auditoría efectiva se requiere de una organización que cuente con la capacidad de implementar las recomendaciones y oportunidades de mejora que sean

determinadas a futuro por los y las auditoras, se requiere entre otros, que la organización beneficiaria cuente con los recursos administrativos, humanos y tecnológicos necesarios para ello. Por lo que la selección de la organización no es un tema menor.

### 3.3.2. Por qué es importante

Con base en las experiencias previas de auditoría adelantadas por Fundación Karisma y teniendo en cuenta los requerimientos de la metodología de SAFETAG, se ha diseñado una matriz de criterios de selección que debe ser considerada por quienes realicen las auditorías, entre otros, la localización y el área de influencia de la organización, la población con la que ésta trabaja, su situación institucional (es decir, si cuenta o no con registro legal formalizado), su infraestructura tecnológica (dado que sólo será posible considerar a aquellas que cuenten con página web, presencia en línea, etc.), la necesidad y el impacto que tendría la auditoría y la sensibilización que podría generar en la organización y sus miembros.

Llevar a cabo este proceso de selección conforme a los criterios propuestos es importante, no sólo porque asegura que los esfuerzos que demanda la auditoría serán aprovechados y transformados en cursos de acción de mejora por parte de los beneficiarios, sino porque proporcionan una metodología de selección objetiva difícilmente influenciable por factores externos.

### 3.3.3. Materiales que se necesitan

- Documento de descripción de los criterios de selección (*Ver anexo 1*)
- Hoja de cálculo con el resultado de la evaluación de los criterios para las organizaciones estudiadas (*Ver anexo 2*)

## 3.4. CONTACTO INICIAL CON LA ORGANIZACIÓN

### 3.4.1. Resumen

El contacto inicial debe estar dirigido a la persona que represente o esté a cargo de la organización de la sociedad civil seleccionada como beneficiaria del proceso de auditoría. La persona auditora deberá establecer dicho contacto por la vía más efectiva, sea llamada telefónica o correo electrónico, y debe en lo posible, orientarse desde el inicio bajo una actitud de apertura y confianza si es que se trata de una organización con la que no existen lazos previamente establecidos.

En este contacto inicial el o la auditora debe conversar con la organización social sobre la intención de llevar a cabo el proceso de auditoría, en qué consiste, cuánto tiempo tomaría su ejecución, y qué se necesitaría de la organización a grandes rasgos (en términos de tiempos, provisión de información, etc.) aclarando desde el comienzo las condi-

ciones del acuerdo al que se deba llegar y que el propósito principal es el fortalecimiento de la seguridad digital al interior de la misma[4].

Es valioso que en este contacto inicial las personas auditoras logren proveer una idea muy clara de sí mismas (a qué se dedican, quiénes son) en aras de generar confianza, más aún si se trata de una organización con la cual no ha habido lazos previos establecidos.

### 3.4.2. Por qué es importante

Este paso es importante porque depende con quién se establezca el contacto y cómo, se obtendrá o no una respuesta positiva de participación en el proceso de auditoría por parte de la OSC.

En este proceso de contacto inicial, es importante que la parte auditora no pierda de vista los tiempos de reacción al mensaje de contacto inicial, pues puede suceder que no se obtenga respuesta alguna, bien porque la persona contactada ya no hace parte de la organización o bien porque se encuentra de viaje, etc.

### 3.4.3. Materiales que se necesitan

- Mensaje (correo, llamada o mensaje instantáneo) a quien dirige o representa la OSC con la cual se establecerá el contacto inicial
- Números telefónicos de las personas a contactar en la OSC
- Seguimiento al mensaje

## 3.5. ACUERDO DE ENTENDIMIENTO

### 3.5.1. Resumen

El propósito del acuerdo de entendimiento es establecer por escrito un marco de cooperación entre quienes realizan las auditorías y la organización de la sociedad civil seleccionada, bajo el cual las partes llevarán a cabo sus actividades de manera coordinada y mutuamente beneficiosa.

Este acuerdo refleja el compromiso de las partes para realizar las actividades del proyecto de implementación de la metodología basada en SAFETAG.

Ambas partes comparten el interés específico por la completa ejecución y conclusión del ejercicio de auditoría, cuyo propósito es influir en la forma en que las organizaciones de

4 En el caso de las dos auditorías que realizamos para este proyecto de adaptación de SAFETAG a Colombia, las auditorías no requerían de la asignación de recursos por las organizaciones más allá del tiempo que debían dedicar para las actividades relacionadas, tampoco incluían presupuesto para la implementación de la hoja de ruta trazada. Estas condiciones pueden cambiar para otro tipo de proyectos.

la sociedad civil utilizan y diseñan sus herramientas tecnológicas y digitales, además de entender cómo ven y comprenden la tecnología en general.

Con el ejercicio de auditoría se espera ayudar a las organizaciones a mejorar su nivel de entendimiento en seguridad digital y, tras realizar la auditoria exploratoria, generar un plan de trabajo para que, con sus recursos, puedan mejorar sus comunicaciones digitales, sistemas informáticos y comportamientos en materia de seguridad, de acuerdo a sus condiciones organizacionales e individuales.

### 3.5.2. Por qué es importante

Suscribir este acuerdo de entendimiento entre las personas auditoras y la organización de la sociedad civil beneficiaria es importante, pues aclara los términos de las actividades mutuamente beneficiosas, detalla las obligaciones y responsabilidades a cargo de cada una de ellas y los resultados producto de las actividades ejecutadas que deberá entregar la parte auditora a la parte auditada. Teniendo también en cuenta que la ejecución de este proceso de forma inadecuada puede incrementar el riesgo de las organizaciones frente a sus adversarios.

### 3.5.3. Materiales que se necesitan

Modelo del acuerdo de entendimiento (*Ver anexo 3*)

# 4. PARTE UNO: PASOS PREVIOS A LA AUDITORÍA

## 4.1. LECTURA METODOLOGÍA DE RIESGOS

### 4.1.1. Resumen

La metodología de riesgos es un anexo que describe el proceso metodológico de análisis de riesgos basado en SAFETAG con sus adaptaciones, detalla cómo se lleva a cabo el levantamiento del contexto organizacional, cómo se realiza el modelado de riesgos, el análisis de procesos y activos, y cómo completar el análisis de riesgos.

Esta lectura está acompañada de conceptos clave que es preciso que la parte auditora revise y tenga en cuenta en su aplicación durante el proceso de auditoría y elaboración del informe final.

La lectura del anexo de metodología de riesgos y el anexo de la herramienta de riesgos, condiciona sin lugar a dudas la comprensión de todo el proceso por lo que es un paso que no puede omitirse.

### 4.1.2. Por qué es importante

Es importante la lectura de los anexos que se describen más arriba, pues contienen información valiosa sobre el qué y el cómo del proceso de auditoría. Su lectura facilitará la tarea de la parte auditora, sirviendo de guía en una especie de paso a paso para la correcta ejecución de los procesos que siguen.

### 4.1.3. Materiales que se necesitan

- Metodología de riesgos (*Ver anexo 7*)
- Herramienta de riesgos SAFETAG (*Ver anexo 8*)

## 4.2. CUESTIONARIO DE ANÁLISIS DE RIESGO EN SEGURIDAD DIGITAL

### 4.2.1. Resumen

Este cuestionario busca establecer una línea de base sobre las percepciones de riesgo en materia de seguridad digital que tienen diversas organizaciones de la sociedad civil en Colombia.

El formulario contiene cuarenta y seis preguntas que tienen como propósito obtener información con relación a aspectos generales de la organización (funciones, localización, población con la que trabajan, temas que trabajan, financiación que reciben, personal, tipo de contratación, etc.); infraestructura y herramientas digitales (presupuesto dedicado al apoyo de tecnologías, si tienen infraestructura tecnológica propia, qué medios digitales usan, dispositivos que se emplean, etc.); seguridad (existencia o no de copias de seguridad de la información, existencia o no de protocolos de seguridad físico y/o digital, etc.); y riesgos y amenazas (vulnerabilidades percibidas, amenazas que ponen en peligro la seguridad física del equipo de trabajo, etc.).

Es preciso que el director de la organización de la sociedad civil o la persona con la cual se haya establecido contacto -en apoyo de los miembros de la OSC- diligencie el formulario de la manera más honesta y transparente posible, con el ánimo de obtener la información más veraz y cercana a la realidad que enfrentan.

### 4.2.2. Por qué es importante

Esta evaluación es importante porque servirá para hacer un primer examen sobre los riesgos en materia de seguridad digital que enfrenta la organización seleccionada. Esperamos que también sirva para desencadenar una primera discusión sobre estos temas al interior de la organización, suscitar su interés en el tema y motivar su participación en el resto del proyecto.

### 4.2.3. Materiales que se necesitan

- Modelo de cuestionario de análisis de riesgo en seguridad digital (*Ver anexo 9*)

## 4.3. REALIZACIÓN DEL 'OSINT'

### 4.3.1. Resumen

La práctica de la Inteligencia de Fuentes Abiertas u OSINT (del inglés Open Source Intelligence), es la disciplina encargada de la adquisición, tratamiento y posterior transformación en inteligencia de la información conseguida a partir de fuentes de carácter público como prensa, radio, televisión, internet, informes de diferentes sectores y en general cualquier recurso accesible públicamente.

Dentro de esta actividad se realizan búsquedas enfocadas a la organización por parte del equipo auditor de forma previa a la auditoría. Con la finalidad de determinar la cantidad de información disponible en internet relacionada con la organización, sus recursos en internet (página web, servidores, etc...), sus miembros, correos electrónicos, otros medios de contacto -físico o electrónico-, quiénes lo integran, sus actividades, qué redes sociales utiliza tanto la organización como sus miembros, documentos, noticias o

hechos relacionados con la organización disponibles en la web, dónde y quién hace el hosting de los servidores webs y cómo se registraron los dominios (información de host/nslookup y whois dominio e IP).

Esta actividad la lleva a cabo la parte auditora. Puesto que se trata de una búsqueda enfocada cuyos resultados los arrojará el medio de búsqueda, se entiende que no participan de manera alguna los miembros de la OSC en dicho proceso.

### 4.3.2. Por qué es importante

Cada organización es diferente, tanto en su estructura organizacional, su misión, su ubicación y su forma de trabajo. Todos estos factores influyen en los tipos de riesgos a los que se encuentra expuesta la organización, así como los tipos de adversarios, amenazas y vulnerabilidades. Por esta razón es muy importante conocer a la organización auditada lo mejor posible para de esta forma poder orientar efectivamente a la organización en el modelado y análisis de riesgos. Con este ejercicio se pueden determinar vulnerabilidades del manejo de la información de la organización en internet y demostrarles los riesgos asociados a malas prácticas comunes y específicas.

### 4.3.3. Materiales que se necesitan

- Se requiere acceso de la persona auditora a medios como internet, prensa y/o radio
- Presentación OSINT (*Ver anexo 10*)
- OSINT Framework (https://osintframework.com/)

## 4.4. TALLER DE SENSIBILIZACIÓN EN SEGURIDAD DIGITAL

### 4.4.1. Resumen

Este taller tiene como propósito sensibilizar a los miembros de la organización a auditar, sobre los riesgos de seguridad a los que se pueden enfrentar, introducir la metodología de análisis de riesgo y presentar una serie de recomendaciones generales para mejorar la seguridad digital en sus actividades cotidianas.

El taller aborda en su orden explicaciones sobre: el modelo de análisis de riesgo, el funcionamiento de internet, las navegaciones segura, privada y anónima, contraseñas seguras y el uso del gestor de contraseñas, el funcionamiento de la telefonía móvil y el uso de redes sociales.

El principio operativo del taller está basado en el enfoque de Actividad, Discusión, Introducción, Profundización y Síntesis (ADIPS) centrado en adultos, donde la información se presenta por etapas y en una variedad de formatos. De esta manera, muchos de los

módulos del taller comenzarán con una actividad práctica o ejercicios básicos para iniciar la reflexión. A partir de ahí, la discusión se realizará con el apoyo de diapositivas y materiales audiovisuales que ayudarán a presentar, sensibilizar y problematizar los diferentes temas. También se ofrecerán recomendaciones sobre prácticas y estrategias de autocuidado, así como herramientas de seguridad digital.

Aunque el taller no está centrado en la instalación, configuración y uso de herramientas digitales, si el tiempo lo permite, se explorará la posibilidad de practicar con algunas herramientas básicas (ej. gestor de contraseñas).

### 4.4.2. Por qué es importante

Llevar a cabo este taller resulta importante en la medida que aproxima una realidad a miembros de organizaciones sociales que ven este tipo de prácticas alejadas de sus contextos o que simplemente desconocen las capacidades del Estado para vigilar a quienes llevan a cabo actividades de impacto social o trabajo con comunidades de base como líderes y lideresas sociales, entre otros.

El taller además ayuda a identificar adversarios que no son tenidos en cuenta al momento de analizar los riesgos digitales, sensibiliza a los miembros de la OSC acerca de las malas prácticas en seguridad digital, sus riesgos en la red, y les enseña y da herramientas de protección en línea mientras les sugiere el cambio de ciertos malos hábitos.

Una de las ventajas que hemos encontrado de realizar este taller de sensibilización en conjunto con la auditoría es que nos facilita la construcción de confianza con las personas de la organización. A quienes hacen la auditoría les proporciona información valiosa de primera mano de las actividades que realiza la organización, sus prácticas, los problemas que han tenido, el conocimiento que tienen sobre el tema y la disposición de las personas que conforman la organización para seguir algunas de las recomendaciones básicas que se dan.

El taller también es un escenario perfecto para despejar dudas que tengan los integrantes de la OSC y aterrizar los temas a su contexto particular.

### 4.4.3. Materiales que se necesitan

- Taller de sensibilización en seguridad digital (*Ver anexo 6*)
- Guión del taller de seguridad digital (*ver anexo 12*)

# 5. PARTE DOS: LA AUDITORÍA

## 5.1. RESUMEN

El proceso de auditoría según nuestra metodología basada en SAFETAG está compuesto por diversos pasos que se articulan en una visita presencial a la organización de la sociedad civil a auditar.

En dicha visita, quien audite entablará conversaciones abiertas en las cuales sea posible obtener la información que se requiere para llevar a cabo su análisis. Para la visita deben estar disponibles las personas que gestionen los procesos más relevantes de la organización, incluída las áreas financiera y administrativa. También las personas que gestionen o almacenen datos sensibles que estén a cargo de la organización. En organizaciones relativamente pequeñas con estructuras organizativas poco verticales, es conveniente que participen la mayor cantidad de personas de la organización. En organizaciones medianas con más estructura deberán estar disponibles las coordinaciones de áreas o programas misionales, personal administrativo y las personas encargadas de la parte tecnológica si es posible.

## 5.2. ENTREVISTA DE LEVANTAMIENTO DE INFORMACIÓN

Cada análisis describe un ejercicio sencillo que puede en su mayoría, seguirse de la formulación de una serie de preguntas que facilitarán su tarea. Es preciso que en el desarrollo de cada análisis se documenten los resultados, que serán posteriormente vertidos en el informe final de recomendaciones.

Generar confianza con el personal de la organización auditada es primordial. Si no se entabla un sentido de confianza no se podrá conocer las debilidades o problemas de la organización.

De manera individual con los miembros de la organización y de manera conversada, se espera que las personas auditoras obtengan información sobre dónde está la información que maneja la OSC actualmente (en qué dispositivos/ubicaciones físicas), quién tiene acceso (físico, de inicio de sesión, permisos), quién necesita tener acceso para realizar los trabajos de la organización, la manera en que se está protegiendo la información, si está guardada en un lugar adecuado, protegida de hurto, humedad o deterioro, entre otros.

Como resultado de esta actividad y con base en la información consignada en el cuestionario de análisis de riesgo en seguridad digital se debe redactar el contexto organizacional, bajo el cual se hará el modelado de riesgos en la segunda parte del proceso.

### 5.2.1. Análisis de contexto

Este componente permite a la persona auditora identificar el *contexto local y tecnológico* para realizar una auditoría SAFETAG segura y bien informada. Este componente consta de investigación documental, que es recopilada y analizada por el equipo auditor, así como por los aportes de las entrevistas. Para llevar a cabo el análisis de contexto, es preciso que quien audite, invite a los miembros de la OSC a responder con claridad las preguntas.

*Ver Anexo 7 Metodología de Riesgos Capítulo Levantamiento del contexto organizacional.*

**Ejercicio:**

Para llevar a cabo este ejercicio de análisis, se sugiere que la actividad entre la parte auditora y auditada se haga de manera conversada, abierta y transparente. El diálogo facilitará entre ambos la obtención de la información por el primero sin que deba ésta en todo caso, emitir opiniones o juicios sobre las respuestas que vayan formulando los entrevistados. En lo posible, entre mayor sea el número de integrantes de la organización auditada que asista a la sesión, mejor, pues la información obtenida habrá de ser más íntegra y fiel a las prácticas reales al interior de la misma.

Se deben documentar los resultados.

### 5.2.2. Análisis de adversarios

Este componente permite a la persona que realiza la auditoría identificar el *contexto de adversarios* para realizar una auditoría basada en SAFETAG segura y bien informada. Este componente consta de investigación documental, que es recopilada y analizada por el equipo auditor, así como por los aportes de las entrevistas.

Para llevar a cabo el análisis de contexto, es preciso que el o la auditora de manera charlada y abierta con los miembros de la organización, les pregunte y determine los principales adversarios, sus motivaciones y capacidades.

*Ver Anexo 7 Metodología de Riesgos Capítulo Modelado de riesgos, Identificación de adversarios.*

**Ejercicio:**

Con la presencia del mayor número posible de integrantes de la organización auditada, se espera que el personal identifique a los posibles adversarios que puedan atentar o amenazar de manera alguna la misión y objetivos de la organización y sus integrantes.

Quien audite puede formular las preguntas listadas en el anexo, o irlas abordando a manera conversación con los miembros de la OSC.

Como resultado de esta actividad se debe revisar el listado de amenazas y adversarios. La persona auditora deberá verificar la aplicabilidad de cada una de ellas, eliminando lo que sobre o incluyendo lo que determine que hace falta.

Se deben documentar los resultados.

### 5.2.3. Análisis de amenazas

Este objetivo utiliza una variedad de actividades para identificar posibles atacantes, accidentes, descuidos, juntando información de fondo sobre la capacidad de los mismos para amenazar la organización. Consiste en la identificación del historial de amenazas específicas, llevadas a cabo por un atacante, de su capacidad de llevarlas a cabo en la actualidad, y la prueba de que la amenaza tiene intención de usar los recursos en contra del objetivo.

La comprobación de las hipótesis de investigación sobre las amenazas actuales tanto las de la organización, como las de la parte auditora, aseguran que la auditoría está basando su trabajo en evaluaciones precisas de las condiciones que enfrenta la organización y de que se están realizando las consideraciones operacionales de seguridad informadas.

Una mayor apropiación del proceso por el personal ofrecerá la oportunidad de explorar su panorama y se comprometerá aún más en el tratamiento de las amenazas identificadas una vez que la auditoría se haya completado.

Los ejemplos de amenazas se encuentran desarrollados de forma extensa en los Anexos.

*Ver Anexo 7 Metodología de Riesgos Capítulo Definiciones.*

*Ver Anexo 8 Herramienta de riesgos SAFETAG pestaña Amenazas.*

**Ejercicio:**

Con la presencia del mayor número posible de integrantes de la organización auditada, se espera que el personal explore las amenazas que ha enfrentado en el pasado reflexionando en torno a cómo se han afectado o podrían afectar los recursos técnicos, físicos y humanos de la OSC. Se deben documentar los resultados.

### 5.2.4. Análisis de procesos y activos

El mapa de procesos bajo la metodología de SAFETAG está pensada de manera muy simplificada, a manera de diagrama de flujo. El equipo auditor y las personas participantes deben describir los procesos internos de la organización paso a paso.

A medida que los procesos se describen, se espera que se vaya elaborando el mapa de procesos usando círculos para representar individuos, servicios u organizaciones que son parte crítica del proceso, conectándolas con flechas que representen alguna comunicación o intercambio de bienes. Cuando esté finalizado el diagrama, debería ser lo suficientemente claro y fácil de entender por aquellos quienes no participaron en esta fase.

Para llevar a cabo este análisis, es preciso formular preguntas como las que se presentan en el Anexo y a modo de ejemplo las que se introducen en el ejercicio a continuación.

*Ver Anexo 7 Metodología de Riesgos Capítulo Análisis de procesos y activos.*

**Ejercicio:**

Para hacer que el personal identifique las jerarquías y procesos internos de tomas de decisión es preciso contar con el mayor número de integrantes de la organización presentes en esta fase. Será necesario, entre otros, preguntar a cada quien cuál es su cargo, si la organización maneja una jerarquía vertical o el proceso de toma de decisiones es horizontal, y de ser así, cómo se lleva a cabo la gestión de cada área a la que pueda cada integrante estar a cargo y de qué recursos dispone para ejecutar sus labores.

Se deben documentar los resultados.

### 5.2.5. Análisis de vulnerabilidades

El planteamiento de esta metodología no es la de un documento técnico para el descubrimiento de vulnerabilidades. Su finalidad es la de trabajar en conjunto con las organizaciones para que ellas mismas puedan identificar las debilidades dentro de las actividades realizadas al interior de la organización.

De ahí que no se utilizan herramientas técnicas para este levantamiento durante las visitas sino que más bien se intenta crear una conciencia con el personal de la organización a la medida que se realiza el levantamiento de información durante las entrevistas y los talleres. Por otra parte la infraestructura  con visibilidad hacia internet sí es evaluada de forma superficial para determinar los riesgos asociados a estos dispositivos o servicios.

Dentro del modelado de riesgos se realiza un barrido inicial de las vulnerabilidades de la organización, sus amenazas y adversarios. Con la finalidad de tener una visión inicial de las características específicas de la organización y empezar a dar unos conocimientos básicos de riesgos a los funcionarios de la organización.

*Ver Anexo 7 Metodología de Riesgos Capítulo Definiciones.*

*Ver Anexo 8 Herramienta de riesgos SAFETAG pestaña Vulnerabilidades.*

**Ejercicio:**

Para llevar a cabo el análisis de amenazas técnicas y físicas se puede hacer una revisión simple de las instalaciones de la organización o de los equipos técnicos, verificando en compañía de sus integrantes si alguna de las amenazas identificadas han podido o podrán acaecer en algún momento.

### 5.2.6. Evaluación de datos (opcional)

Los archivos sensibles a menudo son almacenados en varios dispositivos con diferentes niveles de seguridad. Una evaluación de los datos permite a la parte auditora recomendar soluciones para el almacenamiento seguro que mejor responda a la evaluación de riesgo y flujo de trabajo que necesite la organización según los resultados que arroja la 'entrevista de levantamiento de información'.

Mientras que la persona que realiza la auditoría tiene una visión de ésto basado en el Acceso a la Red y en el trabajo de Mapeo de la Red, la comprensión y aceptación del personal respecto a qué constituye datos sensibles, ayudará más adelante al cambio organizacional.

Un adversario que obtiene acceso a una computadora portátil, una estación de trabajo o una unidad de copias de seguridad, será capaz de leer o modificar la información sensible del dispositivo, incluso si un miembro del personal ha establecido una contraseña fuerte.

Esto no sólo se aplica a las amenazas de pérdida, robo y confiscación, sino también, a los escenarios de "puntos de control" a los que sólo se podrá tener acceso por unos pocos minutos. Además, en el caso de un robo o incursión a una oficina, un adversario podría obtener toda la información sensible en los dispositivos de la organización, posiblemente sin ser detectados. Dispositivos tales como:

- Discos duros
- Memorias USB
- Discos externos
- Celulares
- CDs & DVDs
- Buzones de correo
- La 'nube': Dropbox, Google Drive, etc.
- Copias físicas en la oficina
- Multimedia: Cintas, grabaciones de audio, tarjetas de memorias con fotos/videos, etc.

**Ejercicio:**

En esta actividad se debe crear un mapa de los diferentes puntos donde se encuentra la información al interior de la organización.

## 5.3. POR QUÉ ES IMPORTANTE

La obtención de información de manera presencial y conversada directamente entre la parte auditora y las personas integrantes de la organización de la sociedad civil, facilita establecer un diálogo más natural en el que se pueda determinar con mayor extensión o precisión el contexto de la organización en términos de seguridad digital. Con la información recolectada con el cuestionario así como el OSINT se puede direccionar la conversación hacia los puntos críticos identificados.

## 5.4. MATERIALES QUE SE NECESITAN

- Metodología de riesgos SAFETAG (*Anexo 7*)
- Herramienta análisis de riesgos SAFETAG (*Anexo 8*)
- Cuaderno y esfero

# 6. PASO TRES: INFORME DE AUDITORÍA Y SOCIALIZACIÓN

## 6.1. RESUMEN

La elaboración del informe de auditoría es el paso siguiente a la conclusión del primer y segundo paso de aplicación de la metodología basada en SAFETAG. La información que contiene debe relacionarse de manera clara y entendible, bajo una narrativa descriptiva que permita luego a los miembros de la organización de la sociedad civil auditada, entender plenamente cuáles han sido los hallazgos, cuáles las oportunidades de mejora, y cómo centrar los esfuerzos para llevar a cabo acciones de cambio según sus propios recursos y capacidades y cómo medir los beneficios que trae implementar las mejoras.

## 6.2. POR QUÉ ES IMPORTANTE

La elaboración del informe de auditoría así como la reunión de su socialización con los miembros de la organización auditada es importante. El informe permitirá llegar al conocimiento de los aspectos que constituyen oportunidades de mejora a cargo de la organización; proveyendo igualmente una visión de las tareas a ejecutar para incrementar su propia seguridad, reduciendo a la par vulnerabilidades y riesgos.

No hay que subestimar el tiempo de redacción del informe como tampoco hay que ignorar el lenguaje en que se redacte, que deberá ser lo más claro y sencillo posible. Además es importante tener en cuenta el lenguaje incluyente y el lenguaje que maneja cada organización por su temática.

## 6.3. QUE VAN A APRENDER LOS PARTICIPANTES

La parte auditora, aprenderá a relacionar, redactar y documentar hallazgos y recomendaciones según los resultados del modelado de riesgos y la información recabada en la etapa preliminar a la auditoría. Aprenderá además, a proveer la información sobre las oportunidades de mejora, en un lenguaje claro y comprensible para la organización auditada.

## 6.4. ELABORACIÓN DEL INFORME DE AUDITORÍA

En dicho escrito, es preciso consignar la información obtenida en cada etapa del proceso previo y de auditoría. Su diseño puede estar guiado por los mismos acápites en que se

desarrolla cada una de las dos fases anteriores, y deben en lo posible, tener el mayor nivel de detalle en torno a los resultados obtenidos en los ejercicios propuestos en el proceso de modelado de riesgos.

## 6.5. SOCIALIZACIÓN DE LA AUDITORÍA

El informe de auditoría por sí solo no es de mayor valor para las organizaciones, ya que puede ser un documento muy técnico y extenso. La persona auditora líder debe preparar una presentación de los hallazgos más significativos encontrados incluyendo las tablas de las matrices de riesgos y de las recomendaciones. Se debe preparar de tal manera que lo pueda entender una persona sin conocimientos técnicos y recordando momentos específicos dentro de la visita realizada a la organización. Tenemos que recordar que nuestro objetivo no es asustar a las organizaciones sino presentarles mejoras y mitigaciones a los riesgos encontrados.

La socialización se debe realiza con una reunión virtual o presencial según sea el caso. A la cual debe asistir el contacto principal y las personas que hagan parte de la dirección de la OSC para presentar los hallazgos y explicar las recomendaciones. Siempre tenemos que tener en cuenta la retroalimentación de la organización y en dado caso que se requiera hacer los cambios sugeridos al informe.

Esta reunión debe ser el punto de partida para la creación de la hoja de ruta de la organización. Si bien la auditoría no llega hasta allá, la revisión de las recomendaciones en conjunto con la OSC les permite priorizar y lograr crear una ruta base.

## 6.6. MATERIALES QUE SE NECESITAN

- Modelo de Informe de auditoría (*Anexo 11*)
- Herramienta análisis de riesgos SAFETAG (*Anexo 8*)
- Informe de auditoría impreso y/o digital (según sea el caso)
- Presentación de la tabla de recomendaciones
- Cuaderno y esfero

# 7. ANEXOS

Cada uno de los anexos es un documento por sí mismo que puede consultarse en la dirección respectiva.

Para facilitar su consulta, puede acceder a una carpeta que los contiene en el siguiente enlace https://tinyurl.com/yd75yzon

**Anexo 1.** Criterios de selección organizaciones de la sociedad civil a ser auditadas https://tinyurl.com/yb5ogzkt

**Anexo 2.** Hoja de cálculo de selección de organizaciones de la sociedad civil a ser auditadas https://tinyurl.com/y8bvprun

**Anexo 3.** Modelo de acuerdo de entendimiento https://tinyurl.com/yalv3syt

**Anexo 4.** Taller de metodología SAFETAG https://tinyurl.com/y93kxfhr

**Anexo 5.** Presentación de vigilancia de las comunicaciones en Colombia https://tinyurl.com/ycvx5gz9

**Anexo 6.** Taller de sensibilización en seguridad digital https://tinyurl.com/yb2apbfh

**Anexo 7.** Metodología de riesgos https://tinyurl.com/y8yo82jt

**Anexo 8.** Herramienta de riesgos https://tinyurl.com/ya5xorh8

**Anexo 9.** Modelo de cuestionario de riesgos en seguridad digital https://tinyurl.com/y9ttxy7g

**Anexo 10.** Presentación sobre cómo hacer el OSINT https://tinyurl.com/y9ghma4d

**Anexo 11.** Modelo de informe de auditoría https://tinyurl.com/ydbreqkc

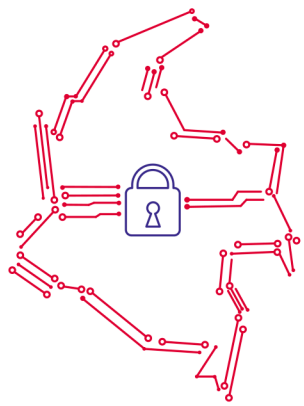
**Anexo 12.** Guión taller de seguridad digital https://tinyurl.com/y7vorl3a

# Currículo para personas auditoras de seguridad digital

## Una propuesta de ajuste a la metodologia **SAFETAG** en Colombia

**Autores**
Pilar Sáenz
Santiago Hernández
Lucía Camacho

**Colaboradores**
Brian Venera
Cristian Torres
Andrés Restrepo
Stéphane Labarthe
Christian Peñaranda



**karisma.org.co**
Twitter: **@Karisma**
Facebook: **@fundacionkarismaa**