Universidad CENFOTEC

Maestría en Ciberseguridad

Documento final de Proyecto de Investigación Aplicada 2

Tema:

Evaluación de los niveles de fuga de datos producidos a través de metadatos contenidos en documentos de acceso público que están disponibles en sitios Web de Instituciones Públicas en Costa Rica.

Estudiante:

Hernández Porras, Salatiel

Julio, 2018

DECLARATORIA DE DERECHOS DE AUTOR

DEDICATORIA

A:

Mi familia, quienes han sabido comprender el sacrificio de trabajar, estudiar y sobre todo, el aceptar que no he podido dedicar el tiempo suficiente para ellos en estos años.

Dios, que eres quien me guía y me da las fuerzas cada día para salir adelante.

Para ustedes con mucho amor…

AGRADECIMIENTOS

A:

Dios, por permitirme cumplir esta meta y haberme dado salud para otro de mis objetivos, además por su infinita bondad y amor.

Mi familia, por haberme apoyado en todo momento, por sus consejos, sus valores, por la motivación constante que me ha permitido ser una persona de bien, pero más que nada, por su amor.

La Universidad CENFOTEC por darme la oportunidad de estudiar y ser un profesional.

Al tutor del proyecto el Sr. Luis Naranjo Zeledón y a don Rodrigo Calvo Solano profesor, colega y amigo, a ellos por su esfuerzo y dedicación, quienes con sus conocimientos, experiencia, paciencia y motivación ha logrado en mí, que pueda culminar mis estudios con éxito.

Son muchas las personas que han formado parte de mi vida profesional, a las que me encantaría agradecerles su amistad, consejos, apoyo, ánimo y compañía en los momentos más difíciles de mi vida. Sin importar en donde estén quiero darles las gracias por formar parte de mí, por todo lo que me han brindado y por todas sus bendiciones.

Para ellos: Muchas gracias y que Dios los bendiga.

RESUMEN EJECUTIVO

El trabajo desarrollado se basa en “Evaluar los niveles de fuga de datos producidos a través de metadatos contenidos en documentos de acceso público disponibles en sitios web de instituciones públicas de Costa Rica” para lo cual se realizó primeramente una revisión bibliográfica de información existente.

Esta revisión bibliográfica permitió conocer información generada por autores que de algún modo han abordado esta temática. Además, conocer conceptos y fundamentos de seguridad de la información utilizados para la prevención de fuga de datos, así como, presentar una recopilación de normativas y legislación existente en materia de seguridad de la información que contribuye con la prevención de esta problemática.

Posteriormente, se presentan los datos obtenidos de los instrumentos aplicados a profesionales de seguridad informática, ciberseguridad y tecnologías referentes a conocer la importancia que se le da a la fuga de datos en las instituciones públicas de Costa Rica, así como, cuales son las principales causas de que ocurra este tipo de incidentes o vulneraciones en estas entidades.

Finalmente, se presentan mecanismos y herramientas utilizados para la limpieza de metadatos en documentos y, un modelo de seguridad que permita prevenir la fuga de datos producida a través de metadatos.

Palabras claves: Fuga de datos, metadatos, fuga de información.

TABLA DE CONTENIDO

Índice de Tablas

Índice de figuras

CAPITULO I

INTRODUCCIÓN

1.1 Generalidades

Actualmente, la seguridad informática ha tomado especial importancia, dadas las cambiantes condiciones y nuevas plataformas de computación disponibles. La posibilidad de interconectarse a través de redes, sistemas, bases de datos y obtener de esto la información deseada ha abierto nuevos horizontes por explorar más allá de las fronteras nacionales, hecho que ha llevado a la aparición de nuevas amenazas en las tecnologías de información.

Esto ha provocado que muchas de las organizaciones orienten a sus usuarios en el uso adecuado de herramientas tecnológicas. A su vez, giran recomendaciones para obtener el mayor provecho de estas; y de esta forma evitan el uso indebido que podría ocasionar serios problemas en los bienes y servicios que prestan las instituciones y, lo que resultaría más agravante, en la información que almacena y utiliza cada una de ellas.

Se podría decir, que la información es un activo muy importante con el que cuenta una organización, pero es el tratamiento que se le da el elemento diferenciador entre cada una de ellas. A raíz de esto, se deberían implementar mecanismos de seguridad que protejan la información, para prevenir filtraciones o fugas de datos y, por ende, que eviten una situación que afecte el prestigio de la institución.

La información constantemente está expuesta a diversos intereses y objetivos que buscan obtenerla para su beneficio, razón por la cual se pretende

realizar una investigación que aborde el tema de la evaluación de los niveles de fuga de datos producidos a través de metadatos.

Cabe destacar que la fuga de datos e información constituye una de las amenazas a nivel de seguridad más peligrosas que puede impactar una institución actualmente. Si no se le da la importancia que amerita, puede exponer servicios críticos e información sensible (nombres de usuario, contraseñas, direcciones, números de teléfono, e-mail) contenidos y almacenados en un documento, una aplicación o servidor, de una determinada institución, lo cual resultaría muy atractivo para intereses de terceros inescrupulosos.

De tal modo las estrategias y recomendaciones que se puedan dar en esta área contribuirán a que se generen nuevos conocimientos que permitan aplicar mejores prácticas en la gestión de la seguridad y, a su vez, permite que se preserven la confidencialidad, integridad y disponibilidad, pilares en los cuales se fundamenta la seguridad de la información.

En este documento se tratará de abarcar desde los aspectos básicos que forman el concepto de datos, información y metadatos hasta el tema de la fuga de datos, riesgos existentes, aspectos que favorecen el que se dé un incidente por fuga de información y, por último, los aspectos de prevención, detección y defensa contra la fuga de datos que se produce a través de metadatos. Estas consideraciones deberían ser atendidas por los encargados de darle tratamiento a los datos, así como por quienes deben atender aspectos relacionados con la seguridad de la información.

Con este proyecto de investigación se pretende concienciar al lector acerca de la importancia de conocer e implementar medidas de seguridad que permitan disminuir el riesgo de sufrir incidentes por fugas de información y, con ello, colaborar con la seguridad de la institución en general.

1.2 Antecedentes del problema

En el transcurso del tiempo ha surgido gran cantidad de avances tecnológicos que han contribuido al desarrollo de nuestra sociedad. Estos avances se dan en muchos ámbitos y se podría decir que tienen un factor común, como lo es la utilización de las Tecnologías de Información y Comunicación (TIC).

Pero, aunque las TIC cada vez más son parte de nuestra sociedad (economía, cultura y en gran medida el desarrollo) e influencian, transforman y mejoran procesos, tramites y otras actividades, no todas las personas por el momento son parte de este proceso de cambio.

Estos adelantos y nuevos mecanismos que se desarrollan traen consigo que a lo interno de las instituciones se considere y se dé mucha mayor importancia a entornos y aspectos que no resultaban tan relevantes en el pasado, como lo son: la seguridad informática, integridad, confidencialidad, disponibilidad, tratamiento y fuga de datos, uso seguro de la información, entre muchos otros.

Pero de la mano con estos nuevos avances y aspectos, para las instituciones resultará de mucha importancia contemplar medidas de seguridad que permitan atender todo lo relativo a estas nuevas temáticas, y que se empiecen a orientar esfuerzos enfocados a prevenir, detectar, contener y, de ser posible, hasta erradicar una situación inesperada. De esta forma, se podrá garantizar que no existan vulnerabilidades que expongan los datos o información. Por tanto, resulta fundamental y determinante que se realicen acciones y esfuerzos en materia de seguridad en estos nuevos escenarios y entornos.

Sin embargo, por el constante crecimiento y utilización de las TIC hay riesgos que pueden afectar a estas nuevas tecnologías y, a raíz de esto, resulta necesario considerar novedosos mecanismos de protección para estas tecnologías. Por ello, resulta necesario que, a la par de cada nuevo servicio o tecnología que se desee utilizar, se contemple por parte de las instituciones todas

las acciones y esfuerzos necesarios en asegurar que estas tecnologías operen de la mejor forma posible.

Cabe destacar que es muy importante para las instituciones que se dé un servicio novedoso y ágil, pero además que sea seguro para quien lo utilice. En este sentido, la seguridad informática, la protección de datos, entre otros, son conceptos primordiales por considerar. Pero no solo las empresas e instituciones son quienes deben tomar en cuenta aspectos de seguridad dentro de su organización; también le corresponde a las personas usuarias el preocuparse porque el tratamiento que se realiza a su información sea el correcto.

A las instituciones les corresponde tomar acciones tendientes a asegurar que por debilidades o fallos en el tratamiento hecho a la información no se revelen y conozcan datos que puedan ser utilizados por personas malintencionadas o con intereses dañinos para la institución.

Por esta razón, se consideran dentro del ámbito de la seguridad aspectos técnicos, físicos y administrativos, que permiten a quienes realizan tratamiento de datos un adecuado manejo y utilización de estos.

La seguridad como tal y la protección de los datos son temas muy novedosos e importantes que se tienen que considerar. Por ello se pretende desarrollar un documento que dé a conocer la importancia que tiene y que le dan a la fuga de datos en las instituciones, y los esfuerzos realizados para prevenirla, pero además busca desarrollar una propuesta de seguridad, la cual permita a quien no actúa de la mejor forma tener una visión más global de la problemática que ocurre y de la importancia que se le debe dar al tratamiento de datos y a una posible fuga de información que se pueda producir en la institución.

Además, esta investigación reviste de importancia porque las instituciones públicas en Costa Rica no atienden el tema de metadatos contenidos en documentos de acceso público.

1.3 Definición y descripción del problema

1.3.1 Planteamiento del problema

Para desarrollar el proyecto se pretende realizar una recopilación de investigaciones y publicaciones producidas entre los años 2008 y 2016 a nivel mundial, que tengan como propósito exponer la problemática que podría causar la fuga de datos producida a través de metadatos contenidos en documentos de acceso público, ya sea porque el problema no se atiende correctamente, porque existe desconocimiento en esta área o porque no se consideran acciones para atender esta situación por parte de las instituciones públicas.

Las investigaciones que se utilizaron abordaron como su principal tema de desarrollo los siguientes aspectos: fuga de datos y de información, protección y tratamiento de datos, todo lo anterior para obtener un conocimiento y aprendizaje que permita el desarrollo de un modelo de seguridad para atender esta problemática, prevenirla y, de ser posible, hasta disminuir el riesgo de que ocurra este tipo de incidentes, contribuyendo así con la seguridad de la institución en general.

1.3.2 Problema general

El proyecto “Evaluar los niveles de fuga de datos producidos a través de metadatos contenidos en documentos de acceso público disponibles en sitios web de instituciones públicas de Costa Rica” se iniciará con una revisión de información en Internet, utilizando en especial los buscadores Google, Yahoo, Bing y Duckduckgo, herramientas que permitirán extraer diversos tipos de aportes e insumos que posibilitarán la realización del trabajo.

A través de Internet se pretende acceder a bibliotecas virtuales (nacionales y extranjeras), repositorios de información, revistas, documentales, libros, proyectos de graduación (tesis) y demás documentación pertinentes, con el propósito de identificar la documentación e investigaciones más relevantes y actuales de autores que han abordado esta temática.

Esta identificación de debilidades que presentan las instituciones permitirá poner en evidencia situaciones de riesgo que existen en torno a este tema de fuga de datos, y que hacen necesario para las instituciones conocer conceptos y fundamentos de seguridad de la información utilizados para la prevención de fuga de datos, así como los principales mecanismos de protección de datos existentes. Por otra parte, se analizarán las principales causas de la fuga de datos y se realizará una recopilación de normativas y legislación en materia de seguridad de la información que contribuyen en la prevención de esta problemática.

Como aporte final, se pretende diseñar un modelo de seguridad para la prevención de fuga de datos a través de metadatos, basado en normas y buenas prácticas de seguridad de la información como ISO, COBIT y normativa nacional e internacional. Esto con la finalidad de crear conciencia sobre situaciones que se podrían presentar y, además, contribuir en el proceso de formación y atención en esta área tan relevante en la actualidad como es la protección de datos o información.

1.3.3 Descripción del proyecto

El proyecto consiste en desarrollar un modelo que permita mejorar la seguridad de la información y específicamente el tema de fuga de datos. Para lograrlo, es necesario evaluar los niveles de fuga de datos producidos a través de metadatos contenidos en documentos de acceso público disponibles en sitios web de instituciones públicas de Costa Rica.

Dichas acciones no solo ayudarán a conocer la importancia que se le da a la fuga de datos en las instituciones públicas, sino que también permitirá conocer las principales causas de la fuga de datos para mejorar la seguridad de la empresa y proporcionar un modelo de seguridad basado en las buenas prácticas que propicien la prevención de fuga de datos a través de metadatos.

Así, el proyecto pretende contribuir con la prevención y protección de la fuga de datos y dar a conocer medidas preventivas y correctivas que se pueden

utilizar. Además, permitirá desarrollar un modelo que permita a las instituciones mejorar en esta área.

1.4 Justificación

En la actualidad, con el avance tecnológico y el uso constante de las comunicaciones electrónicas se ha facilitado muchísimo el poder transmitir la información, pero esta facilidad de comunicación viene de la mano de la necesidad de dar protección y asegurar los datos que se trasmiten, así como los nuevos entornos en los que nos comunicamos. Además, es necesario concienciar sobre el uso correcto que se le debe dar a la información y de los peligros que puede ocasionar para la institución el uso incorrecto o desinteresado de estos medios.

Ante todos estos escenarios, resulta de mucha importancia tomar acciones que permitan proteger la información y disminuir el riesgo de que ocurra algún suceso que pueda generar un impacto negativo en la organización.

Por fácil y amigable que parezca un nuevo producto tecnológico, el uso de la tecnología representa un riesgo para la institución, por lo cual resultará necesario contemplar aspectos y nuevos escenarios en los que se pueda generar fuga de datos a la institución.

La fuga de datos se puede generar en múltiples contextos, ya sea por la sustracción de documentos (papelería, libros, actas), equipos como computadoras, dispositivos móviles (teléfonos, tabletas), por descuido, negligencia y hasta por algún hecho o suceso intencional que se realice predeterminadamente.

Por ello, resulta necesario también conocer cuales consideraciones siguen las instituciones para atender el tema de protección de datos y en especial el de fugas de información.

De tal modo, este trabajo pretende generar conciencia sobre la importancia que tiene la información y los datos para las personas, pero además de lo

descuidados que quizás somos al utilizarlos, así como de lo importante que es para terceros conocer detalles de nosotros, nuestras empresas y de nuestro personal.

Además, es importante realizar una evaluación de la cantidad de datos que por diversas circunstancias están expuestos en sitios web por medio de documentos públicos y que se podrían recopilar para ser utilizados en diversos escenarios y para múltiples propósitos,

Actualmente, muchas instituciones le prestan mayor importancia a la seguridad de la información, destinando para ello personal, herramientas, aplicaciones, etc. Pero en muchos casos no son suficientes estos esfuerzos y se descuidan aspectos sencillos en apariencia pero que pueden resultar muy críticos y sensibles si son obtenidos por terceros con intereses muy perfilados.

Así, es importante que se dé a conocer que normativa y recomendaciones en el ámbito legal existen para prevenir y proteger la fuga de datos. Por tal motivo, aunque exista alguna reglamentación al respecto muchas veces esta no es del todo clara o no es aplicada por todos los sectores de la misma forma y en ocasiones del todo no se considera.

1.5 Viabilidad / Factibilidad del proyecto

En la guía para realizar estudios de factibilidad y pertinencia de programas educativos, Ponce (2002) define el estudio de factibilidad como:

> *“El proceso a través del cual se miden distintos aspectos de posible éxito de un proyecto y el producto que genera. Es usado para ayudar en la decisión de seguir adelante o no, con un proyecto. Generalmente tiene el objetivo de demostrar la factibilidad del proyecto desde un punto de vista social, técnico y económico”. (p. 5)*

Factibilidad se refiere a la disponibilidad de los recursos necesarios para llevar a cabo las metas o los objetivos señalados. Generalmente, la factibilidad se determina sobre un proyecto. Podría incluir los objetivos, alcances y restricciones sobre el sistema, además de un modelo lógico de alto nivel del sistema actual (si existe). A partir de esto, se crean soluciones alternativas para el nuevo sistema, analizando para cada una de éstas diferentes tipos de factibilidades.

1.5.1. Punto de vista técnico

El estudio técnico:

> *"Busca determinar si es posible, física o materialmente, hacer un proyecto, determinación que es realizada generalmente por los expertos propios de área en la que se sitúa el proyecto".(Sapag, 2007, p. 22)*

Este proyecto resultaría factible técnicamente, debido a que en Costa Rica las instituciones públicas utilizan comúnmente un sitio web como mecanismo o herramienta para comunicar e informar a clientes, usuarios, proveedores, entre otros. A su vez, otro de los propósitos es colocar documentación de diversos formatos (.doc, .pdf), para que pueda ser accedida por sectores de interés y público en general. Estas actividades buscan responder a necesidades propias de las instituciones, al desarrollo de las Tecnologías de Información y Comunicación (TIC) y a servicios que ofrecen, lo cual satisface todos los requerimientos necesarios para el desarrollo de la presente investigación.

1.5.2 Punto de vista operativo

Se refiere a la disponibilidad en el momento y en el lugar adecuado, de los recursos humanos que habrán de participar en el proyecto, principalmente cuando éste se convierta en resultados y debe ser operado a través de esos recursos.

Para este proyecto se identificaron todas las actividades que son necesarias para alcanzar el objetivo principal, pero también se les solicitará a

entidades gubernamentales e instituciones públicas de Costa Rica, con quienes se va a trabajar, el apoyo y la disponibilidad para poder utilizar la información (aunque esta sea considerada de acceso público) para el desarrollo de este trabajo final de graduación.

Además, el tema de investigación constituye un posible problema de seguridad, tratamiento y fuga de datos, que podría afectar a instituciones públicas en Costa Rica, y que constituye una debilidad que se acrecienta con el paso del tiempo, y que resulta necesario considerar por la importancia que tiene y que se le debe dar en la actualidad a la protección de los datos y a la prevención de una posible fuga.

1.5.3 Punto de vista económico

El estudio financiero busca definir:

"(…) mediante la comparación de los beneficios y costos estimados de un proyecto, si es rentable la inversión que demanda su implementación." (Sapag, 2007, p 23)

Se refiere a que se dispone del capital en efectivo y de los requerimientos necesarios para invertir en el desarrollo del proyecto, además de que sus beneficios a obtener son superiores a los costos en los cuales se incurrirá al desarrollar e implementar el proyecto o sistema.

La presente investigación resultaría factible, al ser la fuente primaria de investigación documentos de acceso público, siendo necesario contar con el acceso a ellos por medio de un sitio web y, a partir de esto, verificar si se puede obtener información o datos que nos sean de interés para quien acceda a la información (público meta), pero que constituyan un parámetro a ser considerado como fuga de datos, por lo que tendrá así una factibilidad económica asegurada para su pleno desarrollo.

También será un factor por considerar, la cantidad de horas de consultoría que se dedicará al desarrollo de este documento.

1.6 Objetivos

1.6.1 Objetivo general

Evaluar los niveles de fuga de datos producidos a través de metadatos contenidos en documentos de acceso público disponibles en sitios web de instituciones públicas de Costa Rica.

1.6.2 Objetivos específicos

a) Describir los conceptos y fundamentos de seguridad de la información utilizados para la prevención de fuga de datos, así como los principales mecanismos para prevenir la fuga de datos existentes.

b) Conocer la importancia que se le da a la fuga de datos en las instituciones públicas en Costa rica.

c) Elaborar una recopilación de normativas y legislación en materia de seguridad de la información que contribuyen en la prevención de fuga de datos en Costa Rica.

d) Analizar las principales causas de la fuga de datos en las instituciones públicas.

e) Diseñar un modelo de seguridad para la prevención de fuga de datos a través de metadatos en las instituciones públicas, basado en las buenas prácticas de seguridad de la información.

1.7 Alcances y limitaciones

A continuación, se exponen alcances y las limitaciones para la ejecución del proyecto que tiene como finalidad “evaluar los niveles de fuga de datos que se producen a través de metadatos contenidos en documentos de acceso público disponibles en sitios web de instituciones públicas de Costa Rica”.

1.7.1 Alcances

Los alcances del proyecto son:

- Formular estrategias que conduzcan a mejorar la seguridad de la información ya prevenir la fuga de datos que se produce a través de metadatos.
- Ofrecer a la población en general mecanismos de seguridad orientados a la prevención de fuga de datos a través de metadatos y basado en las buenas prácticas de seguridad de la información.
- Por medio de la recopilación de información bibliográfica obtenida a través de Internet, se mostrarán, durante el desarrollo del documento, los conceptos y fundamentos de seguridad de la información utilizados para la prevención de fuga de datos, así como los principales mecanismos de protección de datos existentes.
- A su vez, mediante consulta y recopilación de información bibliográfica, se conocerán las normativas y la legislación en materia de seguridad de la información que contribuye a prevenir la fuga de datos.
- Producto del análisis de los datos recopilados, se determinará si de parte de las instituciones públicas se aplican mecanismos que atiendan el tema de fuga de datos a través de metadatos.
- Finalmente, como fruto del análisis de los datos recopilados se desarrollará un escenario y se darán a conocer herramientas que permitan a las instituciones públicas de Costa Rica atender la fuga de

datos que se producen a través de metadatos y, de esta forma, determinar los mecanismos de prevención pertinentes que permitan a los profesionales de seguridad de las instituciones atender esta situación.

1.7.2 Limitaciones

Las limitaciones del trabajo son:

- Solo un subgrupo de instituciones públicas de Costa Rica será el objetivo de estudio y, en especial, las que utilicen sus sitios web para mostrar documentación a sus usuarios.
- El estudio se limitará a analizar la fuga de datos que se da a través de metadatos contenidos en documentos (.doc, .txt, .pdf, xls, etc.) de acceso público.
- Busca conocer la importancia que tiene para las instituciones el tema de la fuga de datos, pero solo específicamente a través de metadatos, así como los mecanismos se utilizan para prevenir la ocurrencia de este tipo de incidentes.
- La recopilación de normativas y legislación en materia de seguridad de la información y que contribuye en la prevención de fuga de datos se enfocará en documentos que tengan vigencia y cuyo ámbito de aplicación sea Costa Rica.

1.8 Estado de la cuestión

1.8.1 Generalidades

El presente documento tiene como fin realizar una recopilación de investigaciones y publicaciones producidas entre los años 2008 y 2016 a nivel mundial, las cuales basaron su estudio en temáticas que contribuyan a entender la problemática de la fuga de datos o información que se produce a través de metadatos. Para realizarlo, se utilizó Internet como herramienta para la búsqueda de esta información y en especial los buscadores Google, Yahoo, Bing y Duckduckgo, que permitieron extraer diversos tipos de aportes e insumos pertinentes.

Palabras claves: Fuga de datos, metadatos, fuga de información.

1.8.2 Desarrollo

El presente estado de la cuestión es resultado de una investigación de tipo descriptivo que gira en torno al tema de “fuga de datos o información que se produce a través de metadatos.

Fue necesario centrarse en la recopilación de información referente al tema de estudio, para posteriormente realizar un análisis crítico de ésta, que permita finalmente el abordaje más acertado del tema en cuestión.

Por ende, para la realización de este apartado, se investigó acerca de varios aspectos fundamentales, con el propósito de realizar una primera aproximación a la temática que se pretende abordar.

Los aspectos investigados fueron:

- Fuga de datos.
- Fuga de información.
- Metadatos.
- Tratamiento de datos.

En el desarrollo de este documento, fue transcendental la búsqueda y análisis de los principales estudios hechos sobre el tema de fuga de datos o información, mecanismos para la prevención de la fuga de datos y protección de fuga de datos, con énfasis en documentación bibliográfica publicada entre los años 2008 y 2016, y que abordaron, ya sea de manera total o parcial, este eje temático. Cada uno de los hallazgos encontrados es de suma importancia porque constituyen insumos que orientan y enriquecen la nueva investigación.

Por otra parte, resulta relevante señalar que las investigaciones obtenidas son de diversas subáreas de la computación, entre ellas: protección de datos,

seguridad informática, seguridad de la información, fuga de datos; las cuales corresponden a trabajos finales de graduación (TFG), revistas web dedicadas a investigar y presentar diversas temáticas en áreas como la informática, nuevas tecnologías, seguridad informática, seguridad de la información, protección de datos y temas afines a las tendencias tecnológicas y computacionales en las que se orienta el ámbito productivo, empresarial, profesional y educativo. Además, es importante resaltar que también se han recopilado valiosos aportes de investigaciones realizadas por institutos tecnológicos de investigación y otros organismos internacionales (ONG, CERTS, entre otros.) dedicados a fortalecer y concienciar a la población mundial sobre temas de esta naturaleza.

En los siguientes cuadros se pretende mostrar los diversos documentos informativos que se utilizaron para la elaboración de este apartado, identificando el nombre de la persona o personas sustentantes, el año del estudio, la profesión y las categorías relacionadas con la presente investigación.

Posterior a esto, se dará una descripción básica de los documentos identificados asociados al tema de estudio.

Tabla 1. Investigaciones consultadas

Autor(es) o Autora(s)	Año	Especialidad	Categorías
INCIBE	2015	Protección de datos	Fuga de información
INCIBE	2012	Protección de datos	Fuga de información
García, J.L.; Blázquez J.; Chema Alonso	2011	Seguridad informática/protección de datos	Tratamiento de datos
González, D.; Martínez, A.; Pérez, T.; Zárate, J.	2010	Protección de datos	Fuga de datos

Autor(es) o Autora(s)	Año	Especialidad	Categorías
ISACA	2010	Protección de datos	Fuga de datos

Fuente: Elaboración propia, 2016.

García, J.L.; Blázquez J. y Chema Alonso (2011), En su libro Esquema Nacional de Seguridad con Microsoft, realizan un análisis en donde ofrecen tecnologías Microsoft como alternativa de solución para atender los diferentes lineamientos y recomendaciones de seguridad emitidas por el Esquema Nacional de Seguridad español. Estas deben ser consideradas por los responsables de seguridad de cada administración en España, para cumplir con leyes y regulaciones, así como para garantizar que los derechos de los ciudadanos en ese país se respeten.

Se describe también que “el fin último de la seguridad es la protección de datos” (2011, p. 211), y que la información debe ser clasificada según su importancia para asignarle las medidas pertinentes a cada tipo.

Al mismo tiempo, los autores plantean la importancia que se le debe dar a los metadatos y los mecanismos que se deben seguir para eliminarlos de documentos en lo que no necesitamos que se muestren, ya sea por política de la institución o por protección de datos.

La publicación, además, muestra como uno de sus aportes herramientas y procedimientos que permiten visualizar y extraer esta información de los documentos. Esto genera recomendaciones que se deberían acatar para evitar que información sensible salga de nuestra organización simplemente por descuido a la hora de publicar un documento.

González, D.; Martínez, A.; Pérez, T. y Zárate, J. (2010), a través de su tesina para obtener el título de Licenciado en Ciencias de la Informática, proponen un modelo de seguridad que permita implementar soluciones orientadas a la

prevención de pérdida de datos (DLP) en las organizaciones, lo anterior basado en las buenas prácticas. Para lograrlo se propone apoyarse en las políticas y los procedimientos, así como en la tecnología existente (sistemas biométricos, Gateway´s, Firewall´s, Antivirus, Antispam, Antispyware, filtrado de correo electrónico y soluciones de encriptación de datos). Se vislumbra la atención de la pérdida de datos, pero no se le da importancia específicamente a la pérdida de datos que se pueda producir mediante metadatos.

El Instituto Nacional de Seguridad de España, INCIBE (2015) en su guía de gestión de fuga de información, ofrece un documento que tiene como objetivo ayudar al empresario a conocer los conceptos básicos asociados a la fuga de información, cuál sería el origen y los motivos por los que se pudiera dar, pero enfocada primordialmente en la atención de incidentes que puedan darse bajo esta modalidad. Además, señala cuáles serían las consecuencias y el impacto que pudiera tener este tipo de incidentes si no se consideran y se atienden correctamente.

También, da a conocer y describe el proceso de gestión (atención, seguimiento, tratamiento y prevención) en caso de haber sufrido un incidente de fuga de información.

INCIBE (s. f.) A través de otro documento denominado Protección de la información, expone la importancia que tiene la información en la actualidad y considera relevante, durante cualquier tratamiento de datos que se realice, ofrecerle una adecuada protección.

Presenta también aspectos que se deben considerar a la hora de darle tratamiento a la información y mecanismos y mejores prácticas para proteger este activo tan valioso denominado información.

La Asociación de Auditoría y Control de Sistemas de Información, por sus siglas en inglés ISACA (2010), desarrolla un documento denominado Prevención de fuga de datos. Los autores plantean cómo prevenir la fuga de datos a partir del

uso de tecnologías DLP (Data Loss Prevention) dirigidas a detener la pérdida de información sensitiva.

Según se indica por parte de los autores, el escrito básicamente se enfoca en la ubicación, clasificación y monitoreo de información en reposo, en uso y en movimiento.

Además, mencionan que este tipo de tecnologías no corresponden a una solución tipo “plug and play”, sino que necesita de un alto grado de preparación, así como el debido mantenimiento continuo para que pueda funcionar de manera correcta. Mencionan y recomiendan también que la utilización de los DLP puede reducir de manera considerable el riesgo para la organización.

Otros documentos que se consultaron para el estudio son los siguientes:

Tabla 2. Publicaciones web consultadas

Autor o autora	Año	Especialidad	Categorías
Cnnexpansion.com; PCworld.com.mx	2016	Protección de datos Incidentes de seguridad	Fuga de información / Robo de datos
Pagnotta, A.	2016	Protección de datos Incidentes de seguridad	Fuga de información
El país.com	2015	Protección de datos Incidentes de seguridad	Fuga de información / Robo de datos
García, J.	2015	Protección de datos Incidentes de seguridad	Fuga de información / Robo de datos
Gutiérrez, C.	2015	Protección de datos	Fuga de información
Cordero, C.	2014	Protección de datos	Fuga de información
Fisher, D.	2014	Protección de datos	Metadatos
Ruiz, C.	2014	Seguridad informática	Protección de datos

Autor o autora	Año	Especialidad	Categorías
Cebrian, R.	2013	Protección de datos	Fuga de datos
Bortnik, S.	2010	Protección de datos	Fuga de información
Chema Alonso	2009	Protección de datos	Metadatos
Cisco SystemInc	2008	Seguridad informática	Fuga de información / Robo de datos
Clearswift	s.f.	Seguridad informática / Protección de datos	Fuga de información / Robo de datos
Calvo, A.	s.f.	Protección de Datos	Fuga de información

Fuente: Elaboración propia, 2016.

Con relación a las publicaciones web como noticias, artículos y demás documentos encontrados y que se relacionan al tema en cuestión se consideran los siguientes:

Pagnotta, A. (2016), en un artículo que lleva como título ¿Sabes qué es la Haxposición? muestra las últimas tendencias y peligros que se pueden dar si no se atiende por parte de las empresas el tema de seguridad y el de fuga de información.

Este artículo, además, hace referencia al Informe de Tendencias 2016 (Security Everywhere), que muestra entre otras cosas “la cantidad robos de datos mediante ataques informáticos y las consecuencias de la divulgación pública o filtración de esos datos”,(p. 30) combinación de elementos de donde se deriva el término haxposición. En este documento elaborado por el desarrollador de soluciones de seguridad ESSET (2016),específicamente en el apartado número 6, trata el tema de la haxposición como una amenaza emergente que podría tener importantes implicaciones, y que además expone a quien la sufre a la exposición

de secretos corporativos y de empleados inocentes. También, considera cuáles serían las implicaciones de la Haxposición y que podría suceder a futuro si no se toman las consideraciones necesarias para atender esta situación.

Bortnik, S. (2010) presenta un documento titulado Qué es la fuga de información, en donde define este concepto, así como algunos ejemplos de este tipo de incidentes y el objetivo que tienen quienes lo realizan. Así mismo, se mencionan estudios recientes que analizan el tema del costo que tiene para las empresas el que le ocurra este tipo de sucesos.

Calvo, A. (s.f.) desarrolla un artículo denominado Fuga de información, la mayor amenaza para la reputación corporativa, en donde muestra la importancia que tiene para las empresas proteger la reputación. Se enfoca en evitar que se presenten fugas de información debido a que generan una mala imagen y según lo indica la autora representan quizás el mayor costo para una organización, razón por la que se debe atender y considerarse como prioritario este tema.

Cisco System Inc. (2008), publica un documento de nombre Fuga de datos a nivel mundial: Riesgos y errores comunes de los empleados, que sirve para mostrar el estudio que realizó la empresa InsightExpress, entidad contratada por ellos para que investigara usuarios y profesionales de distintos países, con la finalidad de conocer cómo actúan y qué conductas ponen en riesgo la seguridad de los datos personales y empresariales, todo con la finalidad de tomar acciones que prevengan el que ocurra una fuga de información a futuro.

Chema Alonso (2009) publica en su blog una noticia titulada Esquema Nacional de Seguridad: Metadatos, en donde básicamente expone la finalidad que tendrá el Esquema Nacional de Seguridad para España y, específicamente y de forma resumida, la importancia de la limpieza de los metadatos en documentos, aspectos que se contemplarán en el esquema anteriormente mencionado.

Cordero, C. (2014), en su artículo “Fuga de datos impacta marcas, pero empresas carecen de tecnología para enfrentar crisis de imagen” tiene como

objetivo dar a conocer la necesidad que se tiene a nivel empresarial de considerar el tema de la fuga de datos. Pero, además, el autor busca que se potencie el uso de herramientas tecnológicas para atender y mejorar el tema del daño a la reputación que puede generarse por una fuga de datos.

Ruíz, C. (2014), desarrolla una noticia denominada “75% de las empresas de Costa Rica sufrieron al menos un incidente de seguridad informática en 2013”. En esta se exponen los resultados de una investigación realizada que muestra la problemática que se presenta en Costa Rica en el año 2013.Y es que según lo expone el autor, un 75% de las empresas en Costa Rica sufrieron al menos un incidente de seguridad durante el año 2013.

A raíz de esto, Pérez (2013) recomienda crear un grupo cuyo trabajo principal sea proteger la información y luego implementar procesos para la vigilancia de datos en las instituciones.

Cebrián, R. (2013) publicó un estudio realizado por la empresa Eleven Paths denominado Fuga de información en empresas líderes en Data Loss Prevention. En este se presenta el resultado de una investigación que tiene como objetivo meta a instituciones que según se muestra en GarnerInc[1] representan empresas líderes en materia de desarrollo de soluciones para la prevención de fuga de datos (DLP).

Al ser empresas encargadas de desarrollar tecnología para prevenir la fuga de datos, se les analizó la cantidad de metadatos que tenían expuestos a través de documentos públicos. Posterior a esto, se presentaron los resultados, así como los tipos de datos que se encontraron.

La investigación permitió demostrar que no se toma en consideración la fuga de datos a través de metadatos, pero además demostró lo crítico que resulta para las instituciones el que se presente un incidente por fuga de datos, y que este

[1]**Gartner Inc.** es una empresa líder en consultoría e investigación. Fundada en 1979, tiene sus oficinas centrales en Stamford, Connecticut, EE.UU. Cuenta con 7.600 asociados, entre ellos más de 1.600 analistas de investigación y consultores y tiene clientes en 90 países. Fuente: http://www.gartner.com/technology/about.jsp

tipo de incidentes puede ocurrir por diferentes escenarios o como se dice en el documento “la fuga de información puede producirse a diferentes niveles y a través de muchos frentes” (p. 1) y uno de ellos son los metadatos.

Quizás este estudio es uno de los pocos que se asemeja al objetivo que pretende abarcar el desarrollo de esta investigación, pues busca tener como público meta los documentos de acceso público que se encuentran en los sitios web de instituciones públicas en Costa Rica.

Gutiérrez, C. (2015), en el artículo titulado 10 años de fuga de información: conoce los incidentes para no repetir la historia, muestra la cantidad de datos e información que se pierde a causa de la fuga de información. Además, se muestra que entre 2011 y 2015 “casi se duplicó el número de registros filtrados de los seis años anteriores”. Gutiérrez (2015) permite visualizar la tendencia al crecimiento en este tipo de actividades y la importancia de que se considere como prioritaria la atención de esta problemática en cada institución.

Fisher, D. (2014), en una publicación denominada Estudio muestra lo altamente sensibles que son los metadatos en los teléfonos, detalla los resultados de una indagación realizada por investigadores del Laboratorio de Seguridad y Sociedad de la Universidad de Stanford, quienes mostraron los resultados de un programa llamado *“MetaPhone”,* diseñado para la recopilación de metadatos de voluntarios que utilizaban teléfonos celulares Android.

De la información obtenida en la investigación se llegó a la conclusión por parte del grupo de especialistas que los metadatos si son capaces de arrojar información sensible, por lo que resulta indispensable que sean considerados por las instituciones.

El país.com (2015), publicó una nota cuyo título fue Un ciberataque afecta a millones de funcionarios de Estados Unidos. En esta se describe por parte del diario electrónico un ataque de piratas informáticos contra la agencia gubernamental que recopila la información personal de los trabajadores federales

(OPM). Describe que el incidente pudo dejar al descubierto los datos de cuatro millones de empleados, exempleados y contratistas. Y aunque la incursión fue en el mes de diciembre, hasta abril y en mayo se determinó que afectaba a millones de datos personales. Por ello, se puede deducir que este tipo de incidentes es de muy difícil investigación y los resultados se dan a conocer posterior al estudio realizado, sin determinar si se les avisa a los clientes o usuarios de la situación ocurrida. Según este medio informativo, entre los datos robados podría encontrarse información personal y los números de la seguridad social, que identifican a millones de estadounidenses y sirven para realizar todo tipo de gestiones en la vida cotidiana.

Cnnexpansion.com y PCworld.com.mx (2016), publicaron una noticia sobre el robo de datos de aproximadamente 30,000 empleados del FBI. Según esta nota, mediante el uso de una cuenta comprometida (técnica de ingeniería social), piratas informáticos filtraron en total más de 30 mil datos personales de empleados del departamento de seguridad Nacional (DHS, por sus siglas en inglés) de Estados Unidos. Los datos que publicaron incluyeron nombre, teléfono, email y puesto de trabajo.

Garcia, J. (2015, en una noticia titulada Vodafone sufre un ataque donde acceden a datos de cerca de 2000 clientes, presenta la confirmación del ataque informático producido a la empresa Vadafone, en la cual se reportó el robo de unos 20000 datos bancarios de sus clientes. De este ataque se obtuvo, por parte de los cibercriminales, información confidencial sobre estos, incluyendo nombre, fecha de nacimiento, número de móvil y datos bancarios

Vodafone no ha sido la única compañía telefónica que ha sufrido estos ataques. Empresas como TalkTalk también han sufrido este tipo de incidentes y afectaron a más de 1,2 millones de usuarios según este medio informativo.

1.8.3 Resultado final del estado de cuestión

Las investigaciones obtenidas de diversas fuentes permiten evidenciar que la problemática de la fuga de datos en instituciones va en aumento y con el tiempo surgen nuevas formas de incidentes como el de haxposición por mencionar uno, que buscan obtener información de terceros para diversos objetivos.

Se deduce también que, aunque existen compañías que realizan algunos esfuerzos, la documentación encontrada demuestra que en su mayoría los artículos están enfocados en prevenir la ocurrencia de este tipo de situaciones y en concientizar a la población de los peligros y riesgos que representa. Se hace especial referencia a la necesidad de procesos de concientización, prevención e implantación de soluciones de tipo DLP (Data Loss Prevention) en las instituciones.

Además, los resultados obtenidos permiten demostrar que el tema que se propone para esta investigación es considerado por muy pocas instituciones a nivel mundial, que en Costa Rica no se lograron encontrar estudios realizados enfocados en este tema y que del mismo son muy pocos los artículos, documentos, noticiarios, entre otros, que exponen algún tipo de investigación o que dedican algunas líneas para atender y recomendar soluciones basadas en un tipo específico denominado fuga de datos a través de metadatos.

Por otra parte, se desea señalar que se indagó sobre aquellas investigaciones que abordaron, en la medida de lo posible, como su principal eje fuga de datos y de información, metadatos, mecanismos para la prevención de la fuga de datos y tratamiento de datos; sin embargo, se reconoce que pueden existir trabajos que dediquen algún capítulo a ese tema, los cuales son difíciles de localizar, tanto por el sistema de información de las bibliotecas, o bien porque dicho eje no quedó explícito en las palabras claves o títulos con los que se ingresan en ellos.

CAPÍTULO II

MARCO CONCEPTUAL

2.1. Introducción

El motivo del presente trabajo es dar a conocer los aspectos teóricos más importantes, como marco referencial del tema de estudio, que aparte de las definiciones tiene una clara inclinación hacia la fuga de datos, seguridad de la información, metadatos y describe la manera en que se relacionan con el estudio realizado.

2.2. Orígenes del término seguridad

La seguridad es una necesidad básica y como tal, desde épocas anteriores, ya se comenzaba a contextualizar estos conceptos.

Como lo cita Borghello (2001):

> *"Los primeros conceptos de seguridad se evidencian en los inicios de la escritura con los Sumerios (3000 a.c.) o el Hammurabi (2000 a.c.)".* (p. 2)

También la Biblia, Cicerón, Homero o César han sido autores de obras en donde aparecen ciertos rasgos de la seguridad en la guerra y el gobierno.

Como todo concepto, la seguridad se ha desarrollado y ha seguido una evolución dentro de las organizaciones sociales. La sociedad se conformó en familias y esto se convirtió en un elemento limitante para huir. Se tuvieron que concebir nuevas estrategias de intimidación y disuasión para convencer al atacante de que las pérdidas eran inaceptables contra las posibles ganancias.

Según Borghello (2001):

“La primera evidencia de una cultura y organización en seguridad madura aparece en los documentos de la república (estado) de Roma Imperial y Republicana” (p. 2).

Y además indica que:

“El próximo paso de la seguridad fue la especialización. Así nace la seguridad externa (aquella que se preocupa por la amenaza de entes externos hacia la organización; y la seguridad interna (aquella preocupada por las amenazas de nuestra organización con la organización misma)”. (p. 3)

Desde el punto de vista técnico, la seguridad está en manos de la dirección de las instituciones, así como en cada uno de los usuarios y en el grado de concientización respecto a la importancia de la información y el conocimiento que se maneja y al que se tiene acceso.

2.3 Seguridad de la información

La información es un activo importante y esencial en una organización para la toma de decisiones y, como consecuencia, necesita ser protegida adecuadamente.

La información puede existir en muchas formas. Puede estar impresa o escrita en un papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, pero cualquiera que sea la forma que tome la

información o medio por el cual sea almacenada o compartida, siempre debiera estar apropiadamente protegida.

La seguridad de la información es la protección de los datos de un rango amplio de amenazas para poder asegurar la continuidad del negocio y minimizar el riesgo. Se logra implementando un adecuado conjunto de controles, incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware. Para ello, se necesita establecer, implementar, monitorear, revisar y mejorar estos controles cuando sea necesario para asegurar que se cumplan los objetivos.

2.3.1. Resguardo de la información

El resguardo de información consiste en proteger la información y respaldarla en caso de una falla. Hacer una copia de seguridad o copia de respaldo permite restaurar un sistema después de una pérdida de información, daños por virus, accidentes en los equipos, daños en discos duros, o eliminación accidental de la información.

2.3.2. Respaldo de la información

El respaldo de la información implica obtener una copia de los datos en otro medio diferente al que fueron creados, de tal modo que a partir de dicha copia sea posible restaurar el sistema al momento de haber realizado el respaldo. Por lo tanto, los respaldos deben hacerse con regularidad, con la frecuencia preestablecida y de la manera indicada, a efectos de hacerlos correctamente.

2.3.3. Recuperación de la información

La recuperación de la información es la tarea que se lleva a cabo cuando es necesario volver al estado de la aplicación al momento del último respaldo. A partir de los datos de la última copia realizada, se hace una copia en sentido nuevo, recuperando la aplicación.

La recuperación es una tarea eventual. Solo se hace si se han perdido datos, en una magnitud tal que justifique utilizar el respaldo. Puede hacerse en forma parcial, por ejemplo de solo un archivo o completo.

Si se hace una recuperación parcial, debe asegurarse de que no se altere la integridad de los datos.

2.4. Objetivo de la seguridad informática

Para comenzar el análisis de la seguridad informática se deberá conocer las características de lo que se pretende proteger: la información.

2.4.1Dato

Murdick (2010) lo define como:

"Un conjunto básico de hechos referentes a una persona, cosa o transacción. Incluyen cosas como: tamaño, cantidad, descripción, volumen, tasa, nombre o lugar" (p. 157)

O'Brien por su parte menciona que la data usualmente no es útil hasta que está sujeta a un proceso de valor añadido:

- Su forma es agregada, manipulada y organizada.
- Su contenido es analizado y evaluado.
- Es puesta en un contexto para el usuario humano.

Según Martínez (2014), que cita a su vez a Burch (2008):

"Los datos son hechos aislados y en bruto, son el elemento principal de la información"(p.1)

Menciona, además, que existen dos tipos de datos:

1. Datos cuantitativos: aquellos que se pueden contar o medir.
2. Datos cualitativos: aquellos que únicamente pueden describirse.

Existen algunas operaciones básicas que se pueden realizar sobre los datos como:

- Recolección de datos (captación): obtención de datos antes de ser procesados o almacenados, puede ser manual (formatos, documentos) o mecanizada (teclado, mouse, cámara).
- Verificación de los datos (validación): proceso de verificación y corrección de datos durante la captura o después, con la finalidad de minimizar el número de errores.
- Almacenamiento: consiste en guardar los datos previamente capturados en un medio de almacenamiento.
- Recuperación: proceso mediante el cual se logra extraer datos almacenados en un medio.
- Reproducción: generar información procesada para un determinado uso.

D'Ambrosio (2006) menciona que:

"La importancia de los datos, está en su capacidad de asociarse dentro de un contexto para convertirse en información. Por si mismos los datos no tienen capacidad de comunicar un significado y por tanto no pueden afectar el comportamiento de quien los recibe. Para ser útiles, los datos deben convertirse en información para ofrecer un significado, conocimiento, ideas o conclusiones". (p. 157)

2.4.2. Información

Según Senn(1990):

"La información son conocimientos basados en los datos a los cuales, mediante un procesamiento, se les ha dato significado, propósito y utilidad." (P. 33)

La Real Academia Española (2017) define como información privilegiada aquella que:

"por referirse a hechos o circunstancias que otros desconocen, pueden generar ventajas a quien dispone de ella". (p. 1)

En términos generales, hablamos de información como un conjunto de datos que están organizados y que tienen un significado. La información es un elemento fundamental en el proceso de la comunicación, ya que tiene un significado para quien la recibe, que la va a comprender si comparte el mismo código que quien la envía. Esto puede ocurrir del mismo modo en un proceso social, así como en un ambiente computarizado.

Existe Información que debe o puede ser pública y otra que debe ser privada y es por estas razones que es necesario maximizar los esfuerzos para preservarla de ese modo, reconociendo los siguientes aspectos importantes en la información:

- Es crítica: es indispensable para garantizar la continuidad operativa.
- Es valiosa: es un activo con valor en sí misma.
- Es sensitiva: debe ser conocida por las personas que la procesan y sólo por ellas.

Además de los aspectos anteriores, también resulta necesario considerar los siguientes aspectos que la identifican y le generan el valor y la importancia que tiene.

- La integridad de la Información: consiste en determinar si se han alterado los datos durante la transmisión (accidental o intencionalmente).
- La disponibilidad u operatividad de la información: El objetivo de la disponibilidad es garantizar el acceso a un servicio o a los recursos.
- La privacidad o confidencialidad de la información: consiste en hacer que la información sea ininteligible para aquellos individuos que no estén involucrados en la operación.
- El control sobre la información: garantizar el acceso a recursos únicamente a las personas autorizadas.
- La autenticidad de la información: es el acto de establecimiento o confirmación de algo (o alguien) como auténtico, es decir, que reclama hecho por, o sobre la cosa son verdadero.

También, según Senn (1993):

“La información posee atributos que la hacen identificable y valiosa, mismos que se describen brevemente a continuación:

Exactitud: La información puede ser cierta o falsa, exacta o inexacta (aunque puede haber matices entre estos dos extremos).

Forma: La forma es la estructura que tiene la información en el momento en que ella se presenta al receptor. La forma tiene dimensiones de cuantificabilidad, nivel de agregación y medio de presentación.

Frecuencia: La frecuencia de la información es la medida de cuán a menudo se le requiere, reúne o produce.

Alcance: Este concepto es la amplitud de acción de los acontecimientos, lugares, personas y cosas que representa la información.

Origen: El origen de la información es la fuente de la que ésta se recibe, recopila o produce.

Horizonte: La información se puede referir a situaciones o eventos pasados (información histórica), presentes (información actual) o futuros (información proyectada).

Relevancia: La información es relevante si una persona la necesita en una situación particular de toma de decisiones o de resolución de un problema.

Completitud: Si un determinado conjunto de información indica al usuario todo lo que necesita saber en relación con una situación en particular, se dice que es completo.

Oportunidad: La información puede estar disponible o no para el momento en que se necesite". (p. 21-24)

2.4.3. Riesgo

Ya sea que se trate de actos naturales, errores u omisiones humanas y actos intencionales, cada riesgo podría ser evitado o minimizado de las siguientes maneras:

- Minimizando la posibilidad de su ocurrencia.
- Reduciendo al mínimo el perjuicio producido, si no ha podido evitarse que ocurriera.
- Diseño de métodos para la más rápida recuperación de los daños experimentados.

- Corrección de las medidas de seguridad en función de la experiencia recogida.

2.4.4. Daño

Es el resultado causado por la amenaza.

2.4.5 Amenazas

Representa el tipo de acción que tiende a ser dañina y podría comprometer un sistema.

Las amenazas siempre existen y son aquellas acciones que pueden ocasionar consecuencias negativas en la operación de un departamento de informática. Pueden ser de carácter físico o lógico, como ser una inundación en el primer caso, o un acceso no autorizado a una base de datos en el segundo caso.

Las amenazas pueden ser analizadas en tres momentos: antes del ataque durante y después de este. Estos mecanismos conformarán políticas que garantizarán la seguridad de nuestro sistema informático.

- La prevención (antes): mecanismos que aumentan la seguridad (o fiabilidad) de un sistema durante su funcionamiento normal. Por ejemplo, el cifrado de información para su posterior transmisión.

- La detección (durante): mecanismos orientados a revelar violaciones a la seguridad. Generalmente son programas de auditoría.

- La recuperación (después): mecanismos que se aplican, cuando la violación del sistema ya se ha detectado, para retornarlo a su funcionamiento normal. Por ejemplo, recuperación desde las copias de seguridad (*backups*) realizadas.

2.4.6. Vulnerabilidades

Son ciertas condiciones inherentes a los activos o presentes en un entorno informático que facilitan que las amenazas que se materialicen llevan a esos activos a ser vulnerables.

Mediante el uso de las debilidades existentes es que las amenazas logran materializarse, o sea, las amenazas siempre están presentes, pero en la identificación de una vulnerabilidad no podrán ocasionar ningún impacto.

2.4.7 Contramedidas

Son medidas o controles específicos que se aplican y que permiten reducir una vulnerabilidad o amenaza que se presenta.

Es importante que se consideren desde una perspectiva estratégica a nivel institucional, podrían ser pasivas o activas dependiendo de las necesidades, además podrían ser más efectivas y menos restrictivas que un control.

Una contramedida podría ser cambiar el software de un equipo específico por otro que sea por defecto más seguro. Otro ejemplo sería evitar que dispositivos, aplicaciones, o equipos inseguros se conecten a la red institucional.

2.5 Metadatos

Según menciona Senso y Piñero (2003):

> *"La definición de metadatos viene evolucionando desde la década de 1960, fecha en la que el termino fue acuñado por Jack Myers para describir conjuntos de datos. Indican, además, que su primer significado utilizado fue "dato sobre el dato, ya que proporcionaban la información mínima necesaria para identificar un recurso." (p. 97)*

Pero también, porque como lo afirma (Pasquinelli, 1997):

“Los metadatos incluyen información sobre su contexto, contenido y control, así como todo lo que tenga que ver con “el dato.”(p. 98)

Atendiendo a lo anterior, mencionan Senso y Piñero (2003):

“Que a partir de las definiciones que se han ido desarrollado y que surgen con relación a los metadatos se podría considerar que “los documentos (así como sus partes: líneas, párrafos, imágenes...) se pueden tratar como objetos, y los metadatos como los atributos que definen las características de cada uno de ellos, sin limitarse a su descripción simple.”(p. 99)

2.5.1 Importancia

Tras lo expuesto, destacan varias razones que resaltan la importancia de los sistemas de metadatos, las cuales se citan a continuación:

“Incrementan la accesibilidad: la existencia de un conjunto de metadatos que describa correctamente uno o varios objetos aumenta la posibilidad de acceder a ellos (Gilliland-Swetland, 1998).

Disminución del tráfico en la Red: al indizar la representación del objeto, y no el objeto en sí, no requiere demasiado ancho de banda para hacer las búsquedas o generar los índices (Ortiz-Repiso, 1999).

Expandir el uso de la información: ya que facilitan la difusión de versiones digitales de un único objeto.

Control de versiones: se podrán generar diferentes metadatos con distintas cantidades de información sobre un mismo objeto con el fin de distribuirla a un público heterogéneo.

Aspectos legales: los metadatos permiten establecer claramente las restricciones de explotación, informar sobre los derechos de autor, control

> *del uso de todo, o una parte, del objeto, método de pago por su disfrute, controlar el acceso a información restringida...*
>
> *Preservación del objeto original. Tal y como afirman Milstead y Feldman (1999), las búsquedas a través del Web son, en la actualidad, un proceso de equiparación (matching) entre los términos de la consulta y los del documento. Si esa equiparación no se produce (bien sea por un problema en la forma de definir la petición, bien porque esa información sí se encuentra, pero bajo otro concepto que lo describe), el documento no se recuperará. Para estas autoras la utilización de metadatos junto al uso de lenguajes controlados permitiría aumentar la precisión en la mayoría de búsquedas en Internet." (Senso y Piñero, 2003, p. 1)*

Más recientemente, otros autores han destacado la importancia de los metadatos, tal es el caso de Gonzalo (2013), quien indica que:

> *"Los metadatos revelan patrones, relaciones y comportamientos. Su conocimiento afecta nuestra privacidad, y muchas veces puede saberse más a través de ellos que examinando el contenido de esos mensajes, cosa que por otra parte es mucho más complicada e imposible cuando hay cantidades masivas de datos a analizar, sin una muestra específica o limitada." (p. 1)*

Además, a este tipo de información si se le realiza algún proceso de inteligencia puede generar resultados inimaginables que afecten la privacidad y confidencialidad de personas, grupos e instituciones.

Como lo indica Felten (2013)[2], citado a su vez por Gonzalo(2013), se puede usar el siguiente ejemplo hipotético[3] de la información que se podría obtener a través de los metadatos:

> *"Una mujer joven llama a su ginecólogo; luego inmediatamente llama a su madre; luego a un hombre, con quien, durante los últimos meses ha estado hablando por teléfono repetidamente por las noches después de las 23hs; seguido de una llamada a un centro de planificación familiar que también ofrece abortos."(p.1)*

Y como lo indica Aranda (2013) refiriéndose al párrafo anterior:

> *"El historial que sale de ahí muestra más evidencias incluso que la grabación del contenido de una llamada telefónica".(p. 1)*

Por su parte, en esa misma declaración Felten (2013) citado a su vez por Gonzalo (2013) destaca aún más la importancia que pueden tener lo metadatos cuando menciona,

> *"Los patrones de llamadas pueden revelar cuándo estamos despiertos o durmiendo, nuestra religión, si una persona regularmente no hace llamadas los sábados, (el día santo o día de descanso judío), o si hace una gran cantidad de llamadas en Navidad, nuestros hábitos de trabajo y*

[2]Edward W. Felten. Profesor de informática y de Relaciones Públicas, así como Director del Centro de Política de Informática, en la Universidad de Princeton. Licenciatura en Física en el Instituto de Tecnología California en 1985, el grado de Maestría en Ciencias de la Computación e Ingeniería de la Universidad de Washington en 1991, y un Ph.D. en el mismo campo de la Universidad de Washington en 1993.

[3]Ejemplo que fue utilizado por Felten(2013) en su declaratoria(DECLARATION OF PROFESSOR EDWARD W. FELTEN) cuando se le pidiódescribir la importancia que tenían los metadatos, posterior a que se revelara por Edward Snowden algunos de los propósitos que tenía la NSA con la recolección de metadatos de llamadas telefónicas realizadas por los ciudadanos de distintos paices. Todo con la intención de convencer a un juez para conceder una medida cautelar de parar o limitar la actividad de la NSA.

nuestras aptitudes sociales, el número de amigos que tenemos o incluso nuestras afinidades civiles y políticas".

Felten (2013) en su informe además indica:

"Las innovaciones en almacenamiento electrónico hoy en día nos permiten mantener, barata y eficiente, grandes cantidades de datos. La capacidad de conservar los datos de esta magnitud es, por sí mismo, un desarrollo sin precedentes de decisiones sea posible el mantenimiento de una historia digital que anteriormente no estaba dentro del alcance de la mano de cualquier individuo, corporación o gobierno." (p.8)

"Esta capacidad de almacenamiento de datos recién ha dado lugar a nuevas formas de explotar el registro digital sofisticadas herramientas informáticas permiten el análisis de grandes conjuntos de datos para identificar patrones y relaciones incrustados, incluyendo datos personales, hábitos y comportamientos." (p 8)

2.5.2Usos

Como lo indican García, Blázquez y Chema Alonso (2011):

"A través de los metadatos, se puede extraer información tal como el direccionamiento utilizado en una red interna, nombres de usuarios y de servidores, información de versiones de productos y otros datos de carácter crítico" (p. 218)

De ahí la importancia de tratarlos adecuadamente en cualquiera de las categorías.

Los usos y las razones por las que extraen y almacenan los metadatos pueden ser múltiples, por lo que se describirán algunos que se dieron a conocer a nivel mundial por la importancia que tienen.

2.5.2.1 Metadatos de correo electrónico

El *email* representa uno de los medios que más comúnmente se utiliza en la actualidad para la comunicación entre personas, ya sea para temas laborales, educativos o personales. A raíz de esto, un grupo de investigadores del MIT (Massachusetts Institute of Technology) desarrollaron un proyecto denominado Immersion (Smilkov, Daniel; JagdishDeepak; Hidalgo, César, 2013), el cual permite a los usuarios conocer los metadatos de campos como (de, para, fecha y hora) de sus propios correos electrónicos. Todo con el objetivo de conocer los principales contactos y las relaciones que se dan entre quienes se comunican.

A partir de esto se puede conocer quiénes son las personas con las que más se comunican, periodos de tiempo en los que se realizaron determinadas actividades: ir a la universidad, cambios de trabajo, relaciones personales, por mencionar algunas.

2.5.2.2 Metadatos de llamadas telefónicas

Como lo indica Felten (2013):

"El análisis de metadatos a gran escala, puede revelar la red de personas con las que nos comunicamos comúnmente llamado un gráfico social. Con la construcción de un gráfico social que todos los mapas de las llamadas telefónicas de una organización con el tiempo, se podría obtener un conjunto de contactos que incluye una porción sustancial de los miembros del grupo, los donantes, los partidarios políticos, fuentes confidenciales, y así sucesivamente. El análisis de los metadatos que pertenece a esos

abonados individuales, moviendo una "salto" más lejos, podría ayudar a clasificar cada uno, con el tiempo produciendo un desglose detallado de las relaciones de asociación de la organización." (p. 17)

Por ejemplo:

"Los metadatos pueden ayudar a identificar nuestras relaciones más cercanas. Dos personas en una relación íntima pueden llamarse periódicamente", o "una persona que hable esporádicamente es menos probable que sea un amigo cercano que alguien que hable una vez por semana."(p. 217)

2.5.2.3 Metadatos de transporte

Según Chipchase (2008), en la ciudad de Nueva York:

"(…)los taxis equipados con sistemas de posicionamiento global permiten a los funcionarios estudiar los patrones migratorios de taxis amarillos y llegar a mejorar ideas para la ingeniería de tráfico."(p.1)

2.5.2.4 Metadatos en documentos

Comúnmente se utilizan los documentos escritos en formatos (.doc, .pdf) para trasmitir o comunicar información. Pero, ¿a qué situaciones se podría exponer un usuario si recopilaran los metadatos de estos documentos?

Por ejemplo, García, Blázquez y Chema Alonso (2011) indican que los metadatos:

"Pueden suministrar información significativa que pudiera ser utilizada contra la organización." Además mencionan que "la disposición de esta información por parte de personas inapropiadas podría permitir la

realización de un ataque posterior apoyado en información privilegiada o, incluso, dañar la imagen de la organización." (p. 217)

Mencionan, también, que en el año 2003 sucedió una situación relacionada con el gobierno británico que sirve de ejemplo para ilustrar lo anteriormente dicho:

"*Cuando se cernía el comienzo de la guerra contra Irak, Toni Blair presentó un informe en la cámara alta del gobierno británico que había sido recibido del servicio de inteligencia de los Estados Unidos. Dicho informe se presentó como una prueba irrefutable de que en Irak existían armas de destrucción masiva. El presidente fue preguntado repetidas veces si el documento había sido manipulado, modificado o tratado de alguna forma por el gobierno británico y la respuesta siempre fue negativa.*

Sin embargo, el documento se publicó en el sitio web del gobierno sin tener en cuenta los posibles metadatos y la información oculta que pudiera contener. El documento en cuestión había sido escrito en formato .doc, el formato nativo de Microsoft Word, y resulto qué, al hacer análisis de metadatos, apareció una lista de ediciones realizadas por ciertos usuarios que demostraban que el documento sí había sido manipulado por personal del gobierno británico." (p. 217)

Al igual que los ejemplos anteriores se pudiera referir otra gran cantidad de escenarios en donde se utilizan los metadatos, pero lo importante es determinar la importancia que tienen y los múltiples propósitos que tendrían para distintos sectores en la sociedad.

2.5.3 Medidas de seguridad y prevención

2.5.3.1 Limpieza de documentos

El proceso de limpieza de documentos:

“retirará de estos toda la información adicional contenida en campos ocultos, metadatos, comentarios o revisiones anteriores, salvo cuando dicha información sea pertinente para el receptor del documento.” (García, Blázquez y Chema Alonso, 2011, p. 218)

Además, los mismos autores indican que:

“Esta medida es especialmente relevante cuando el documento se difunde ampliamente, como ocurre se ofrece al público en un servidor web u otro tipo de repositorio de información.” (p. 218)

Y se tiene que tener presente que el incumplimiento de esa medida puede perjudicar:

“Al mantenimiento de la confidencialidad de información que no debería haberse revelado al receptor del documento.

Al mantenimiento de la confidencialidad de las fuentes u orígenes de la información que o debe conocer el receptor del documento.

A la buena imagen de la organización que difunde el documento por cuanto demuestra un descuido en su buen hacer”. (p. 219)

La opción de automatización resulta muy interesante, puesto que independiza la seguridad del buen hacer del usuario. Aunque los usuarios sean

conscientes de la necesidad, desafortunadamente se enfrentan a que, en el trabajo diario, esta limpieza no siempre se realiza, o bien no se hace correctamente.

2.5.4 Características

Tabla 3. Características de los metadatos

ATRIBUTO	CARACTERÍSTICAS	EJEMPLOS
Fuente	Metadatos internos generados por el agente creador con el propósito de informar sobre el momento de su creación.	Nombre de ficheros. Estructuras de directorios. Formatos de ficheros y algoritmos de comprensión.
Fuente	Metadatos externos relativos a una información que se modifica después de su creación.	Registros catalográficos. Información sobre sus derechos de autor.
Método de creación	Método generado automáticamente por un ordenador.	Índice de palabras clave. Logs. Weblogs y bitácoras.
Método de creación	Métodos creados manualmente.	Herramientas descriptivas.
Naturaleza	Creados por el autor del documento del objeto.	Los utilizados en las páginas .HTML.

Naturaleza	Generados por profesionales de la información, independientemente de quien sea el autor del documento objeto.	Registros MARC. Encabezamientos de materia.
Estado	Estático: no cambian desde su creación	Título, fecha de creación.
Estado	Dinámico: varía con el uso del documento objeto.	Estructura de directorios. Logs.
Estado	A largo plazo: necesario para asegurarse de que el documento objeto será accesible en todo momento.	Información de los derechos (de autor, de uso, de difusión…)
Estado	A corto plazo: con clara vocación transaccional.	Información sobre el uso.
Estructura	Con estructura basada en estándares.	MARC. TEI. AACR2.
Estructura	Sin estructura predecible.	Metadatos ad hoc (la mayoría de los generados en y para bibliotecas digitales).
Semántica	Normalizados por medio de un vocabulario controlado.	MARC. AACR2.
Semántica	No controlados.	Etiquetas HTML.
Nivel	Colecciones de metadatos relativos a colecciones de documentos objeto.	MARC. Índices especializados.
Nivel	Un metadato relativo a un documento. objeto individual, fuera de cualquier colección.	Información sobre el formato. Leyenda de una imagen.

Fuente: Elaboración propia, 2016.

2.6 Fuga de datos

El Instituto Nacional de Ciberseguridad de España INCIBE (2015), define la fuga de información como:

> *"(…) pérdida de la confidencialidad, de forma que información privilegiada sea accedida por personal no autorizado." (p.5)*

Según la compañía desarrolladora de soluciones de seguridad ESET (2011):

> *"La naturaleza del problema de fuga de datos es originado por dos vertientes principalmente "la primera relacionada con la tecnología, y la segunda con las personas. Esta clasificación obedece a un aspecto fundamental de la información, que es su medio de propagación (sistemas o personas) y el lugar donde se almacena (dispositivos de almacenamiento o la memoria de cada individuo)." (p. 4)*

Con relación a la tecnología indican que puede ocasionarse por diversas razones, entre las que destacan:

> *"La dificultad de administrar y gestionar la enorme cantidad de datos que procesan las organizaciones.*
>
> *El uso de dispositivos (keylogger, pen drive infectado por un malware), que en sus distintas formas y tipos permite acceder a equipos, explotar vulnerabilidades y afectar la privacidad de forma directa.*
>
> *En ocasiones puede darse una fuga no intencional, por deberse a un error técnico que hace que quede expuesta determinada información, ya sea en Internet o dentro de las empresas." (ESET, 2011, p. 5)*

Para enfrentar los problemas derivados del aspecto técnico aparecieron diversos mecanismos. ESET (2011) menciona los siguientes:

> *"Data Loss Prevention (DLP), Data Leak Prevention (también DLP), Information Leak Detection and Prevention (ILDP), Information Leak Prevention (ILP), Content Monitoring and Filtering (CMF) y Information Protection and Control (IPC)."(p. 5)*

Pero hay que considerar que estas tecnologías no funcionan solas, sino que deben ser minuciosamente configuradas, para lo cual se requiere previamente conocer el valor de la información, que se obtiene luego de realizar un estudio de valuación de activos, o bien al menos un reconocimiento de los activos de información importantes, de manera que se reconozca el valor que tiene aquello que se desea proteger.

Más allá de esto, la información se debe clasificar en función de su nivel de requerimientos de confidencialidad, integridad y disponibilidad.

Desde el punto de vista humano, mencionan que

> *"Si bien lo normal no es que una persona desee robar información intencionalmente, no se puede negar que la posibilidad exista." (ESET, 2011, p. 6)*

Además, indican que algunas de las razones por las que podría generarse serían:

- Empleados disconformes con la empresa.
- Malas intenciones.
- El espionaje interno que puede existir por parte de empleados.

- Por interese externos a la institución.
- Por algún fraude o engaño que podrían dejar expuesta la información.

Para enfrentar los problemas derivados del aspecto humano existen alternativas que ESET (2011) menciona: generando registros (logs) que en caso de una auditoria (y que esta sea efectiva) permitan garantizar el uso de los activos de información y su trazabilidad.

Esto implica el conocimiento de la vinculación entre las personas y sus accesos, para que de esta forma se pueda evitar en gran medida la fuga de información. En caso de filtrarse hacia el exterior, se podría señalar de manera directa a todos aquellos que tuvieron acceso y se podría analizar su uso previo al incidente, obteniendo posibles conclusiones y responsables.

Resulta fundamental que exista un alto grado de concientización y que las políticas de seguridad estén correctamente aplicadas para garantizar que quienes manejen información confidencial tengan asumidos los riesgos relacionados con su filtración.

CAPÍTULO III

MARCO METODOLÓGICO

Este capítulo desarrolla la metodología empleada durante el desarrollo de la investigación, la cual que destaca de manera principal que este trabajo es teórico, debido a que la información se obtiene a través de entrevistas, cuestionarios, programas de cómputo, observación directa, indirecta e instrumentos que ayudarán a obtener y constituir al final el producto denominado Evaluación de los niveles de fuga de datos producidos a través de metadatos contenidos en documentos de acceso público disponibles en sitios web de instituciones públicas de Costa Rica.

3.1 Tipo de investigación

La investigación es considerada una actividad humana, orientada a obtener nuevos conocimientos y aplicarla a la solución de problemas o interrogantes de carácter científico.

Investigar es un método que conlleva a esclarecer una inquietud, una satisfacción, un problema.

3.2 Finalidad

Con la implementación de este proyecto se pretende formar las bases a nivel de prevención en seguridad informática y seguridad de la información, que permita a las instituciones considerar aspectos de detección y prevención de fuga de información que podría ocurrir a través de metadatos, procedentes de documentos de acceso público disponibles en sitios web de instituciones.

También se pretende generar y desarrollar una cultura de seguridad de la información en la empresa que permita aplicar mejoras prácticas en las actividades que se realizan diariamente.

De tal manera, la finalidad de este proyecto es del tipo aplicado, ya que busca contribuir en la solución de una problemática que se presenta y que afecta a muchas instituciones debido a malas prácticas realizadas y hasta por desconocimiento de esta.

3.2. Enfoque de la investigación

El presente trabajo utiliza un enfoque mixto (cualimétrico).

De la combinación de ambos enfoques surge la investigación mixta, que incluye las mismas características de cada uno de ellos, según Grinnell (1997), citado por Hernández et al (2003)

> *"Señala que los dos enfoques (cuantitativo y cualitativo) utilizan cinco fases similares y relacionadas entre sí:*
>
> - *Llevan a cabo observación y evaluación de fenómenos.*
> - *Establecen suposiciones o ideas como consecuencia de la observación y evaluación realizadas.*
> - *Prueban y demuestran el grado en que las suposiciones ó ideas tienen fundamento.*
> - *Revisan tales suposiciones ó ideas sobre la base de las pruebas o del análisis.*
> - *Proponen nuevas observaciones y evaluaciones para esclarecer, modificar, cimentar y/o fundamentar las suposiciones ó ideas; o incluso para generar otras." (p. 5)*

El enfoque cualitativo busca comprender los procesos relativos (origen, prevención, detección) a la fuga de datos, ya que según Hernández, Fernández y Baptista (2010):

"(…) la interacción física entre el investigador y el fenómeno suele ser próxima, suele haber contacto". (p. 12)

Además, estos autores, continúan señalando:

"El papel de los fenómenos estudiados (objetos, seres vivos, etcétera) son activos.

La relación del investigador y el fenómeno estudiado son de interdependencia, se influyen, no se separan.

El uso de la teoría es un marco de referencia.

La forma de los datos para analizar es en forma de textos, imágenes, piezas audiovisuales, documentos y objetivos personales."(p. 12)

Por su parte, también utiliza un enfoque cuantitativo porque incluye la recolección y análisis de los datos para que posteriormente se puedan conocer cantidades y tipos de datos que se fugan de las instituciones públicas.

Y como bien lo define Galeano (2004):

"Los estudios de corte cuantitativo pretenden la explicación de una realidad social vista desde una perspectiva externa y objetiva. Su intención es buscar la exactitud de mediciones o indicadores sociales con el fin de generalizar sus resultados a poblaciones o situaciones amplias. Trabajan fundamentalmente con el número, el dato cuantificable." (p. 24)

Y de esta forma Ruiz, Borboa y Rodríguez (2013), considerando las características de ambos enfoques, mencionan que:

“Por una parte el enfoque cuantitativo al utilizar la recolección y el análisis de datos para contestar preguntas de investigación y probar hipótesis establecidas previamente y al confiar en la medición numérica, el conteo y la estadística para establecer con exactitud patrones de comportamiento en una población, y por otra parte, el enfoque cualitativo, al utilizarse primero en descubrir y refinar preguntas de investigación y al basarse en métodos de recolección de datos sin medición numérica, como las descripciones y las observaciones y por su flexibilidad se mueve entre los eventos y su interpretación, entre las respuestas y el desarrollo de la teoría.” (p. 10)

3.3. Diseño de la investigación

El estudio se caracteriza por contar con un diseño investigación-acción.

Según Alvarez-Gayou (2003)

“El propósito de la investigación-acción es resolver problemas cotidianos e inmediatos” (p. 159)

Su propósito fundamental se centra en aportar información que guie la toma de decisiones para programas, procesos y reformas estructurales, además de mejorar prácticas concretas.

A su vez:

“Los principales beneficios de la investigación acción son la mejora de la práctica, la comprensión de la práctica y la mejora de la situación en la que tiene lugar la práctica” (Latorre, 2005, p.27).

3.4 Población y muestreo

3.4.1 Población

La población se define como:

"(…) un conjunto finito o infinito de elementos con características comunes para las cuales serán extensivas las conclusiones de la investigación." (Arias, 2006, p. 81)

Por otro lado Pérez (2009) la define como:

"Conjunto finito o infinito de elementos que se someten a un estudio; pertenecen a la investigación y son la base fundamental para obtener información."(p. 70)

Basados en las anteriores definiciones, la población que se utilizará para esta investigación serán las instituciones públicas de Costa Rica, principalmente quienes utilizan sitios web para publicar documentos que son de acceso público.

Las instituciones que se seleccionaron como muestra son las siguientes:

Tabla 4. Población de la investigación - Ministerios

Ministerio	Área de desempeño	Página web
Ministerio de la Presidencia	Coordinación interinstitucional e interministerial, diálogo entre el Presidente y los poderes del Estado y la sociedad civil.	http://www.presidencia.go.cr
Ministerio de Relaciones Exteriores	Política exterior.	http://www.rree.go.cr/
Ministerio de Agricultura y Ganadería	Producción agrícola y ganadera.	http://www.mag.go.cr
Ministerio de Economía, Industria y Comercio	Gestión económica, comercial e industrial del país.	http://www.meic.go.cr
Ministerio de Ciencia, Tecnología y Telecomunicaciones	Investigación científica y desarrollo tecnológico.	http://www.micit.go.cr
Ministerio de Comercio Exterior	Exportaciones y tratados internacionales de comercio.	http://www.comex.go.cr
Ministerio de Cultura y Juventud	Conservación de patrimonios históricos, administración de teatros, museos y grupos artísticos estatales (Compañía Nacional de Teatro y de Danza, Orquesta Sinfónica Nacional, etc.), actividades culturales y artísticas, área de juventud y gestión de la	http://www.mcj.go.cr

Ministerio	Área de desempeño	Página web
	política pública para la persona joven.	
Ministerio de Educación Pública	Educación básica (guardería, preescolar, primaria y secundaria)	http://www.mep.go.cr
Ministerio de Seguridad Pública	Seguridad pública	http://www.seguridadpublica.go.cr/
Ministerio de Hacienda	Cobro de impuestos y el control de aduanas	http://www.hacienda.go.cr
Ministerio de Justicia y Paz	Control de población penitenciaria, indultos, relación del Poder Ejecutivo con el Poder Judicial	http://www.mjp.go.cr
Ministerio de Gobernación y Policía	Migración, fronteras y policía preventiva	
Ministerio de Ambiente y Energía	Protección del medio ambiente, gestión de parques nacionales y áreas protegidas y fuentes de energía naturales	http://www.minae.go.cr
Ministerio de Obras Públicas y Transportes	Construcción y administración de vías públicas e infraestructura, supervisión de aviación civil, policía de tránsito y puertos	http://www.mopt.go.cr
Ministerio de Salud Pública	Administración de hospitales públicos y la Caja Costarricense de	http://www.ministeriodesalud.go.cr

Ministerio	Área de desempeño	Página web
	Seguro Social, control de las normas de salud en establecimientos públicos y actividades mediante permisos e inspectores, control de epidemias	
Ministerio de Trabajo y Seguridad Social	Supervisión del cumplimiento de las leyes laborales, negociación de huelgas y lucha contra el desempleo.	http://www.mtss.go.cr
Ministerio de Planificación Nacional y Política Económica	Planificación y coordinación interinstitucional	http://www.mideplan.go.cr
Ministerio de Vivienda y Asentamientos Humanos	Dotación de vivienda digna y de interés social, supervisión sobre el Instituto de Vivienda y Urbanismo (INVU) y el Banco Nacional de Vivienda (BANVI)	http://www.mivah.go.cr
Ministerio de Comunicación	Ministerio sin cartera que sirve como enlace entre gobierno y medios de comunicación.	http://www.presidencia.go.cr

Fuente: Elaboración propia, 2016.

Tabla 5. Población de la investigación – Instituciones autónomas

Institución autónoma	Área de desempeño	Página web
Instituto Costarricense del Deporte y la Recreación (ICODER)	Gestión de los espacios públicos deportivos y recreativos, coordinación con los entes internacionales deportivos, promoción del deporte y la recreación	http://www.ider.go.cr
Instituto Costarricense de Turismo (ICT)	Promoción de la industria turística y la imagen del país como destino turístico.	http://www.ict.go.cr
Instituto Mixto de Ayuda Social (IMAS)	Combate a la pobreza y programas de asistencia social (IMAS)	http://www.imas.go.cr
Instituto Nacional de la Mujer (INAMU)	Protección y de defensa de las mujeres, aplicación de las leyes contra la violencia doméstica y la integración de la mujer.	http://www.inamu.go.cr
Instituto Nacional de Seguros (INS)	Seguros	http://www.ins.go.cr
Caja Costarricense de Seguro Social (CCSS)	Salud pública	http://www.ccss.go.cr
Instituto Costarricense de Electricidad (ICE)	Electricidad y telecomunicaciones	http://www.ice.go.cr

Institución autónoma	Área de desempeño	Página web
Banco Central de Costa Rica (BCCR)	Banco Central	http://www.bccr.go.cr
Instituto Costarricense de Acueductos y Alcantarillados (ICAA)	Acueductos y alcantarillados	http://www.aya.go.cr
Instituto de Fomento y Asesoría Municipal (IFAM)	Asesoría a los gobiernos locales	http://www.ifam.go.cr
Instituto Costarricense de Ferrocarriles (INCOFER)	Ferrocarriles	http://www.incofer.go.cr
Instituto Costarricense de Pesca y Acuacultura (INCOPESCA)	Pesca	http://www.incopesca.go.cr
Patronato Nacional de la Infancia (PANI)	Protección de la Niñez	http://www.pani.go.cr
Instituto Nacional de Aprendizaje (INA)	Educación técnica	http://www.ina.go.cr
Instituto Nacional de Vivienda y Urbanismo (INVU)	Construcción de vivienda	http://www.invu.go.cr

Institución autónoma	Área de desempeño	Página web
Refinadora Costarricense de Petróleo (RECOPE)	Hidrocarburos	http://www.recope.go.cr
Instituto de Desarrollo Rural (INDER)	Distribución de tierras	http://www.ida.go.cr
Junta de Protección Social (JPS)	Lotería nacional para reinversión social	http://www.jps.go.cr

Fuente: Elaboración propia, 2016.

3.4.2 Muestra

Según Rena (2010),

"Una muestra es un conjunto de unidades, una porción del total, que representa la conducta del universo en su conjunto."(p. 26)

Para el desarrollo de esta investigación, la muestra estará compuesta por dos instituciones públicas correspondientes a ministerios e igual número (dos) instituciones públicas, pero de carácter autónomo que utilizan sitios web para publicar documentos de acceso público. La selección no es una muestra estadística, sino que se escogió con cierta intencionalidad y afinidad, esto con el propósito de contar con suficientes datos para el análisis.

Tabla 6. Muestra seleccionada para la investigación- Ministerios

Ministerio	*Área de desempeño*	*Página web*
Ministerio de Hacienda	Cobro de impuestos y el control de aduanas	http://www.hacienda.go.cr
Ministerio de Justicia y Paz	Control de población penitenciaria, indultos, relación del Poder Ejecutivo con el Poder Judicial	http://www.mjp.go.cr

Fuente: Elaboración propia, 2016.

Tabla 7. Muestra seleccionada para la investigación- Instituciones autónomas

Institución autónoma	*Área de desempeño*	*Página web*
Caja Costarricense de Seguro Social (CCSS)	Salud pública	http://www.ccss.go.cr
Instituto Costarricense de Electricidad (ICE)	Electricidad y Telecomunicaciones	http://www.ice.go.cr

Fuente: Elaboración propia, 2016.

3.5. Sujetos y fuentes de información

3.5.1. Sujetos

"Los sujetos son todas aquellas personas físicas o corporativas que brindan información". (Barrantes, 2007, p. 92)

Los sujetos seleccionados para el desarrollo de esta investigación son los siguientes:

- Profesional de seguridad informática o seguridad de la información de la empresa.
- Ingeniero en informática de la institución.
- Funcionarios de la institución.

3.5.2. Fuentes de información

Son los medios utilizados para recolectar la información necesaria para la elaboración del proyecto. Se mencionan dos tipos:

"Instancias de donde surgen las ideas de investigación, como materiales escritos y audiovisuales, teorías, conversaciones, creencias, entre otros" (Hernández, 2006 p. 34).

3.5.2.1 Fuentes primarias de la información

Como fuente primaria, se utiliza la información obtenida de la empresa, así como la información corresponde a la entrevista, que se aplica a un profesional de seguridad informática o seguridad de la información, al ingeniero en informática, a los funcionarios de la institución, con el fin de conocer los mecanismos y procedimientos que utilizan para la protección y prevención de fuga de datos.

Además, la observación y el juicio de expertos son otras de las fuentes primarias que nos van a permitir obtener información relevante y de importancia, para generar soluciones y recomendaciones con el fin de poder abordar integralmente el tema del proyecto.

> *"Proporcionan datos de primera mano, pues se trata de documentos que contienen resultados de estudios, como libros, antologías, artículos, monografías, tesis, documentos oficiales, reportes de asociaciones, trabajos presentados en conferencias o seminarios, artículos periodísticos, testimonios de expertos, documentales, videocintas en diferentes formatos, foros y páginas en Internet, entre otros". (Hernández, 2006, p.66).*

3.5.2.2 Fuentes secundarias de información

Este tipo de información se obtiene de páginas de Internet con información complementaria de los conceptos asociados a seguridad de la información, fuga de datos, fuga de información y metadatos.

> *"Son listas compilaciones y resúmenes de referencias o fuentes primarias publicadas en un área de conocimientos en particular, las cuales comentan artículos, libros, tesis y otros documentos especializados". (Hernández, 2006, p. 66)*

3.6. Categorías de investigación

El desarrollo de las categorías para investigar fue el primer paso de esta etapa del proyecto. Estas deben estar estrechamente ligadas con lo establecido en cada uno de los objetivos específicos. En el presente estudio se trabaja en las siguientes estrategias.

3.6.1 Categoría 1

"Describir los conceptos y fundamentos de seguridad de la información utilizados para la prevención de fuga de datos, así como los principales mecanismos de protección de datos existentes".

Definición conceptual

Describe conceptos y fundamentos de seguridad de la información utilizados para la prevención de fuga de datos, así como los principales mecanismos de protección de datos.

Instrumento

- Análisis bibliográfico de documentación existente relacionada con la seguridad de la información, la prevención de fuga de datos, así como los principales mecanismos de protección de datos existentes.

3.6.2 Categoría 2.

"Conocer la importancia que se le da a la fuga de datos en las instituciones públicas en Costa Rica."

Definición conceptual

Conoce la importancia que tiene para las instituciones públicas en Costa Rica, el tema de fuga de datos.

Instrumento

- Entrevistas efectuadas a profesional de seguridad informática y/o seguridad de la información, al ingeniero en informática y a los funcionarios de la institución.
- Observación directa de políticas, normativas y procedimientos enfocados a prevenir la fuga de datos o información.

- Utilización de aplicaciones de software para detectar fuga de información a través de metadatos, procedentes de documentos de acceso público disponibles en sitios web.

3.6.3 Categoría 3.

"Elaborar una recopilación de normativas y legislación en materia de seguridad de la información que contribuyen en la prevención de fuga de datos en Costa Rica".

Definición conceptual

Recopilación de normativas y legislación en materia de seguridad de la información que contribuye a la prevención de fuga de datos.

Instrumento

- Revisión de legislación existente que contribuye en la prevención y detección de fuga de datos.

3.6.4 Categoría 4.

"Analizar las principales causas de la fuga de datos en las instituciones públicas".

Definición conceptual

Analiza las principales causas de la fuga de datos en las instituciones públicas.

Instrumento

- Análisis bibliográfico de mecanismos utilizados por instituciones para prevenir y detectar la fuga de datos.
- Juicio de profesionales expertos en seguridad de la información, que atienden el tema de fuga de datos en sus instituciones.

3.6.5 Categoría 5.

"Diseñar un modelo de seguridad para la prevención de fuga de datos a través de metadatos en las instituciones públicas, basado en las buenas prácticas de seguridad de la información".

Definición conceptual

Modelo de seguridad para la prevención de fuga de datos a través de metadatos en las instituciones públicas, basado en las buenas prácticas de seguridad de la información.

Instrumento

- Análisis bibliográfico de mecanismos utilizados por instituciones para prevenir y detectar la fuga de datos
- Juicio de profesionales expertos en seguridad de la información, que atienden el tema de fuga de datos en sus instituciones.
- Entrevistas efectuadas a profesional de seguridad informática o seguridad de la información, al ingeniero en informática y a los funcionarios de la institución.
- Observación directa de políticas, normativas y procedimientos enfocados a prevenir la fuga de datos o información.
- Utilización de aplicaciones de software para detectar fuga de información a través de metadatos, procedentes de documentos de acceso público disponibles en sitios web.

3.7. Cuadro de categorías

Tabla 8. Definición de las categorías

Objetivo especifico	Categoría	Definición	Instrumento
Describir los conceptos y fundamentos de seguridad de la información utilizados para la prevención de fuga de datos, así como los principales mecanismos de protección de datos existentes.	Conceptos y fundamentos de seguridad de la información utilizados para la prevención de fuga de datos, así como los principales mecanismos de protección de datos.	Describe conceptos y fundamentos de seguridad de la información utilizados para la prevención de fuga de datos, así como los principales mecanismos de protección de datos.	- Análisis bibliográfico de documentación existente relacionada con la seguridad de la información, la prevención de fuga de datos, así como los principales mecanismos de protección de datos existentes.
Conocer la importancia que se le da a la fuga de datos en las instituciones públicas en Costa Rica.	Importancia que tiene para las instituciones públicas en Costa rica, el tema de fuga de datos.	Conoce la importancia que tiene para las instituciones públicas en Costa Rica, el tema de fuga de datos.	- Entrevistas efectuadas a profesional de seguridad informática o seguridad de la información, al ingeniero en informática y a los funcionarios de la institución. - Observación directa de políticas, normativas y procedimientos enfocados a prevenir la fuga de datos o información. - Utilización de aplicaciones de software para detectar

Objetivo especifico	Categoría	Definición	Instrumento
			fuga de información a través de metadatos, procedentes de documentos de acceso público disponibles en sitios web.
Elaborar una recopilación de normativas y legislación en materia de seguridad de la información que contribuye en la prevención de fuga de datos en Costa Rica.	Normativas y legislación en materia de seguridad de la información que contribuye a la prevención de fuga de datos.	Recopilación de normativas y legislación en materia de seguridad de la información que contribuye a la prevención de fuga de datos.	- Revisión de legislación existente que contribuye en la prevención y detección de fuga de datos. - Análisis bibliográfico de mecanismos utilizados por instituciones para prevenir y detectar la fuga de datos. - Juicio de profesionales expertos en seguridad de la información, que atienden el tema de fuga de datos en sus instituciones.
Diseñar un modelo de seguridad para la prevención de fuga de datos a través de metadatos en las instituciones públicas, basado en las buenas prácticas de seguridad de la información.	Prevención de fuga de datos a través de metadatos en las instituciones públicas, basado en las buenas prácticas.	Modelo de seguridad para la prevención de fuga de datos a través de metadatos en las instituciones públicas, basado en las buenas prácticas de seguridad de la información.	- Análisis bibliográfico de mecanismos utilizados por instituciones para prevenir y detectar la fuga de datos - Juicio de profesionales expertos en seguridad de la información, que atienden el tema de fuga de datos en sus instituciones. - Entrevistas efectuadas a profesional de seguridad

Objetivo especifico	Categoría	Definición	Instrumento
			informática o seguridad de la información, al ingeniero en informática y a los funcionarios de la institución. - Observación directa de políticas, normativas y procedimientos enfocados a prevenir la fuga de datos o información. - Utilización de aplicaciones de software para detectar fuga de información a través de metadatos, procedentes de documentos de acceso público disponibles en sitios web.

Fuente: Elaboración propia, 2016.

3.8. Descripción de instrumentos

En esta investigación se utiliza la entrevista, el cuestionario, los programas de cómputo, observación directa y el análisis de contenido como instrumentos de recolección de datos necesarios para el análisis previo y posterior evaluación de los niveles de fuga de datos producidos a través de metadatos contenidos en documentos de acceso público disponibles en sitios web de instituciones públicas de Costa Rica.

3.8.1. Entrevistas

Se selecciona la entrevista como técnica para la recolección de información. Este instrumento de investigación se aplica a un profesional de seguridad informática o seguridad de la información, ingenieros en informática y funcionarios de la institución.

Las entrevistas se basan en la elaboración de preguntas para obtener información de cómo se aborda el tema de la fuga de datos, para así, determinar las debilidades que presentan en la institución referentes al tema en cuestión y que permitan diseñar un modelo de seguridad para prevenir la fuga de datos a través de metadatos en las instituciones públicas, basado en las buenas prácticas de seguridad de la información.

> *"Recopilación de información que se realiza de forma directa, cara a cara y a través de algún medio de captura de datos". (Muñoz, 2002, p. 329).*

3.8.2. Juicio de expertos

Es un conjunto de opiniones que pueden brindar profesionales expertos en una industria o disciplina, relacionadas al proyecto que se está ejecutando.

Al tener este proyecto una connotación técnica, resulta necesario contar con la opinión y la experiencia de profesionales que se dedican al desarrollo de soluciones informáticas orientadas a prevenir la fuga de datos y de profesionales en seguridad informática y de seguridad de la información.

> *"Este tipo de información puede ser obtenida dentro o fuera de la organización, en forma gratuita o por medio de una contratación, en asociaciones profesionales, cámaras de comercio, instituciones gubernamentales, universidades." (Esterkin, 2012, p. 1)*

3.8.3. Programas de cómputo

Se utilizarán aplicaciones de software disponibles, que permitan detectar fuga de información a través de metadatos, procedentes de documentos de acceso público disponibles en sitios web.

3.8.4. La observación

Este instrumento se aplica en las instituciones, principalmente visualizando normativas, políticas y procedimientos existentes elaborados a lo interno de la organización. Para esto se elabora antes una guía que permita la recolección de datos específicos, que sirvan para diagnosticar y formar una línea base de conocimiento, que contribuya a detallar la situación en la que se encuentran, así como las necesidades que pueda tener para que se pueda llevar a cabo dicho proyecto de manera exitosa.

> *"Observar la forma en que ingresan los usuarios al centro de cómputo, a fin de conocer las medidas de seguridad para el acceso" (Muñoz, 2002, p.360).*

3.8.5. Análisis bibliográfico

Se realiza una selección de los datos obtenidos de todas las fuentes de información, con el fin de poder analizar, interpretar y desarrollar los objetivos expuestos de esta investigación.

3.9 Indicadores de evaluación del proyecto

Los indicadores de evaluación del proyecto determinarán la buena marcha del proyecto o, en su defecto, su mala marcha; por eso, debemos prestar mucha atención en el desarrollo del proyecto a los siguientes indicadores:

3.9.1 Participación

La participación es la acción y efecto de participar (tomar o recibir parte de algo, compartir, noticiar). El término puede utilizarse para nombrar la capacidad de

la ciudadanía de involucrarse en las decisiones de un lugar determinado, un país o región.

Es, sin lugar a dudas, la participación el indicador vital para evaluar un correcto desarrollo del proyecto, ya que sin ella no habría proyecto. Algo que sería fundamental es poder involucrar a la mayor cantidad de personas que utilizan a diario los laboratorios y equipos de cómputo y forman parte de la especialidad en informática.

3.9.2 Motivación

Para el desarrollo de este proyecto, la motivación sería un aspecto trascendental a considerar. Esta se basa en aquellas cosas que impulsan a un individuo a llevar a cabo ciertas acciones y a mantener firme su conducta hasta lograr cumplir todos los objetivos planteados. La noción, además, está asociada a la voluntad y al interés. En otras palabras, puede definirse la motivación como la voluntad que estimula a hacer un esfuerzo con el propósito de alcanzar ciertas metas.

Cabe resaltar que la motivación implica la existencia de alguna necesidad, ya sea absoluta, relativa, de placer o de lujo. Cuando alguien está motivado, considera que aquello que lo entusiasma es imprescindible o conveniente. Por lo tanto, la motivación es el lazo que hace posible una acción en pos de satisfacer una necesidad.

3.9.3 Compromiso

Se dice que una persona se encuentra comprometida con algo cuando cumple con sus obligaciones, con aquello que se ha propuesto o que le ha sido encomendado. Es decir, que vive, planifica y reacciona de forma acertada, para conseguir sacar adelante un proyecto, una familia, el trabajo, estudios, entre otros.

Para que exista un compromiso es necesario que exista conocimiento. Es decir, no podemos estar comprometidos a hacer algo si desconocemos los aspectos de ese compromiso, y las obligaciones que supone.

De todas formas, se considera que una persona está realmente comprometida con un proyecto cuando actúa en pos de alcanzar los objetivos por encima de lo que se espera.

3.9.4 Integración

Se trata de la acción y efecto de integrar o integrarse (constituir un todo, completar un todo con las partes que faltaban o hacer que alguien o algo pase a formar parte de un todo).

En todos los casos, la integración siempre supone el esfuerzo coordinado, la planeación conjunta y la convivencia pacífica entre los sectores que conforman el grupo. Esa es la única forma donde las partes pueden constituir un todo, aún sin perder su individualidad.

Por lo tanto, en este proyecto la integración es el eje principal para llevar a cabo todas las acciones necesarias para el logro de los objetivos propuestos en el proyecto.

3.9.5 Seguridad

Se refiere a todo aquello que está exento de peligro, daño o riesgo. La seguridad es un estado de ánimo, una sensación, una cualidad intangible. Se puede entender como un objetivo y un fin que el hombre anhela constantemente como una necesidad primaria.

Por ello, un proyecto que no contemple dentro de sus indicadores este aspecto, se consideraría incompleto y hasta podría poner en riesgo a sus actores y participantes. Además, el hecho de generar un ambiente de seguridad en lugares donde no se le da la importancia que se debe resultaría fundamental y permitirá que

se consideren a futuro dentro de la especialidad técnica estos aspectos como primordiales y de gran relevancia e importancia para la institución.

3.10 Prerrequisitos del proyecto

- Contar con la participación de profesionales de seguridad informática o seguridad de la información, ingenieros en informática y funcionarios de la institución, para con esto lograr las metas planteadas en el proyecto.
- Recopilar información suficiente de cada institución que se utilice en la muestra, para de esta forma poder aproximarnos a la realidad lo mejor posible.
- Contar con los permisos respectivos, para acceder al personal y profesionales requeridos.
- Satisfacer las necesidades que permitan el desarrollo y conclusión del proyecto a partir de los recursos destinados para llevarlo a cabo.

CAPÍTULO IV

ANÁLISIS E INTERPRETACIÓN DE LOS DATOS

4.1. Presentación

En este capítulo, se analizan e interpretan los datos obtenidos mediante los diferentes métodos y técnicas para la recolección de información, de acuerdo con las categorías propuestas.

El cuestionario y la entrevista representan herramientas muy importantes, porque a través de ellas se puede tener acceso a información relacionada con la situación actual que ocurre con el tratamiento y uso de metadatos en las instituciones públicas de Costa Rica, así como de las opiniones de las personas que ahí laboran.

La organización de este capítulo es la siguiente:

1. Se formula la estrategia.

2. El objetivo por el cual se formuló la estrategia.

3. Se enuncia la pregunta.

4. La tabla o gráficos donde se muestran los resultados obtenidos.

5. Análisis e interpretación de los datos.

4.2. Tabulación de los datos

Después de haber aplicado los instrumentos de recolección de datos a personal de seguridad informática, seguridad de la información, tecnologías de información y a los usuarios en general de diferentes instituciones públicas a nivel

nacional, se realizó la tabulación de los datos, analizando los instrumentos antes mencionados para posteriormente presentarlos, ya sea mediante un gráfico o tabla para su respectivo análisis.

4.3. Análisis e interpretación de resultados

Para la realización de este proyecto se aplican como instrumentos el cuestionario y la entrevista, pero además se emplean la observación, el juicio de expertos y el análisis bibliográfico para complementar dicho estudio. Los datos que se analizan e interpretan en este capítulo se obtienen de una entrevista aplicada a profesionales de seguridad informática, seguridad y tecnologías de información y de un cuestionario aplicado a profesionales de esas ramas. Estos instrumentos se enfocan en funcionarios con capacidades para atender el tema de fuga de datos a través de metadatos contenidos en documentos de acceso público, quienes serían las posibles personas con capacidades para tomar acciones para atender esta situación en las instituciones.

La entrevista aplicada utiliza preguntas abiertas y el cuestionario se efectúa con preguntas abiertas y cerradas y de selección múltiple. Para los instrumentos aplicados, se pretende mostrar los resultados, en una tabla o mediante un gráfico que ilustre los datos obtenidos.

A estos datos que se obtienen se les realiza su respectivo análisis e interpretación para conocer los resultados.

4.3.1 Estrategia 1:

Conceptos y fundamentos de seguridad de la información utilizados para la prevención de la fuga de datos que se produce por la existencia de metadatos, así como los principales mecanismos de protección existentes.

Referente a la estrategia 1, se realizó un análisis bibliográfico de información existente relacionada con la prevención de fuga de datos.

Objetivo: Describir los conceptos y fundamentos de seguridad de la información utilizados para la prevención de la fuga de datos que se produce por la existencia de metadatos, así como los principales mecanismos de protección existentes.

Seguridad

Para la RAE[4] (2017), el termino seguro equivale a que esta "Libre y exento de riesgo" (*p.1)* es un "Lugar o sitio libre de todo peligro" (*p.1)*

Pero como es conocido, no se puede hablar de estar 100% seguro o de que se esté libre de todo riesgo; por esta razón, se considera que lo importante es reducir los riesgos hasta llegar a niveles aceptables por la institución.

Información

Es un activo muy importante con el que cuenta la institución y que debe protegerse.

Seguridad de la información

Básicamente se ocupa de la información, independientemente de su formato. Incluye documentos en papel, digital, propiedad intelectual, en la mente de las personas (ideas) y la comunicación verbal o visual.

Además, atiende la preservación de la confidencialidad, la integridad y la disponibilidad de la información.

Principios básicos

[4] Real Academia Española (2017)

- **Confidencialidad:** es la protección de la información de acceso no autorizado o la divulgación. Diferentes tipos de información requieren diversos niveles de confidencialidad y la necesidad de confidencialidad puede cambiar con el tiempo.

- **Integridad:** es la protección de la información de modificación no autorizada.

- **Disponibilidad** garantiza el acceso y uso oportuno y confiable a la información y sistemas cuando una institución lo requiera.

Vulnerabilidad

Según el ESET (2017):

"(…) es una debilidad en un activo o control que puede ser aprovechada por uno o más agentes externos."(p.1)

Amenaza

Es la causa potencial de un incidente no deseado que puede resultar en daños a un sistema u organización. La ISO/IEC 13335 (2013) define una amenaza como:

"Una causa potencial de un incidente no deseado". (p.1)

Ataque

Intento de destruir, exponer, alterar, inutilizar, robar, obtener acceso no autorizado o hacer uso indebido de los activos.

Riesgo

“Es la combinación de la probabilidad de un acontecimiento y su consecuencia.” (Organización Internacional de Normalización y la Comisión Electrotécnica Internacional [ISO/IEC], p. 73). El riesgo se mitiga mediante el uso de controles o medidas de seguridad.

La evaluación de riesgo es una de las funciones más importantes de una organización de seguridad cibernética.

Por lo tanto, entender el riesgo y evaluaciones de riesgo son requisitos críticos para cualquier encargado y profesional de la seguridad.

Fuga de información

Origen y motivos

El origen de las amenazas que provocan la fuga de información puede ser tanto externo como interno. Por origen interno se entienden las fugas de información ocasionadas por empleados propios de la empresa, ya sea de forma inadvertida (por desconocimiento o por error) o a propósito.

Los principales orígenes externos de la fuga de información abarcan desde organizaciones criminales hasta activistas.

Causas

Las causas principales de los casos de fuga de información (y por tanto el carácter de las medidas preventivas que se deberán adoptar) pueden ser clasificadas en dos grupos estrechamente relacionados: aquellas que pertenecen al ámbito organizativo y aquellas que hacen referencia al ámbito técnico.

Organizativas y técnicas

- Falta de una clasificación.
- Falta de conocimiento y formación.

- Ausencia de procedimientos.
- Ausencia de acuerdos de confidencialidad de la información.
- Código malicioso o malware.
- Acceso no autorizado.
- Servicios en la nube para el almacenamiento.
- Tecnologías móviles.

Consecuencias

Las consecuencias de un incidente de fuga de información son el tema de atención en las instituciones y las organizaciones actualmente. Por ello, resulta trascendental comprender las posibles consecuencias para así, brindar una adecuada gestión a los incidentes de este tipo y diseñar una estrategia que permita tomar decisiones y medidas adecuadas para minimizar el impacto del incidente.

Estimación del impacto

Para INCIBE (2016) es necesario estimar el conjunto de las consecuencias que se derivan de un incidente de fuga de información, para lo cual las agrupa en las siguientes categorías:

- **Daño de imagen.** Genera un impacto negativo en la entidad y lleva implícita la pérdida de confianza.
- **Consecuencias legales.** Podrían conllevar sanciones económicas o administrativas.
- **Consecuencias económicas**. Estrechamente relacionadas con las anteriores, se encuentran dentro de aquellas que suponen un impacto negativo a nivel económico, con una disminución de la inversión, negocio, entre otros.

- **Otras consecuencias.** Son aquellas que afectan o suponen un impacto negativo en ámbitos muy diversos, como por ejemplo el ámbito político, diplomático, institucional, o gubernamental, entre otros.

Además, menciona que un factor por considerar es el tipo de organización, siendo diferente si el incidente afecta a la administración (institución pública) o si se trata de una entidad privada.

- **Administración.** En este sector un posible daño a la imagen es un factor que cobra importancia desde un punto de vista político. No teniendo igual importancia, las consecuencias económicas y las sanciones debidas a incumplimiento de la legislación.

- **Entidades del sector privado.** Las consecuencias que tienen mayor peso son aquellas de carácter económico. Por otra parte, un incidente puede suponer la pérdida de confianza de los inversores o de sus clientes, lo que también puede tener consecuencias muy significativas sobre su negocio y su actividad.

Otro de los factores adicionales es si la información que ha sido accedida es considerada como confidencial o no. Las consecuencias pueden ser muy distintas.

- **Información confidencial o restringida.** Aquella información que se considera crítica para los procesos de la entidad. Por ejemplo, datos de clientes, contabilidad y datos de los propios trabajadores.

- **Información no confidencial.** El hecho de su divulgación impactaría la imagen de la empresa, pero el peso del impacto económico será menor.

Para INCIBE (2016):

> *“Considerando estos tres factores podemos tener una aproximación que ayude a determinar las posibles consecuencias de un incidente. Además, enfatiza que, para obtener una escala de valor de las consecuencias, es necesario contar con una valoración objetiva tanto de los factores comentados como de otros factores, siguiendo un procedimiento de análisis de riesgos.”(p.10)*

Contemplando todos los factores citados, podría diseñarse un plan de gestión del incidente de fuga de información, acorde a las necesidades de cada institución.

Seguidamente, se referencian tecnologías que, aunque no atienden directamente la fuga de datos por metadatos, sí permiten que se pueda abordar la fuga de información desde una perspectiva más general en una entidad.

Mecanismos para la prevención de pérdida de datos

Clasificación de la información

Antes de implementar cualquier mecanismo para prevenir la pérdida de datos es indispensable realizar una clasificación de datos e información, y es que como lo indica Peter (2015), citado por Matthee, M (2016):

> *“Es importante considerar que deben existir políticas de información para la empresa. Estas políticas preparan a la organización desde una perspectiva legal y asegura que todos los datos de la empresa se analicen y clasifiquen de manera apropiada”. (p. 14)*

Además, menciona Matthee, M (2016):

“Las herramientas automatizadas de clasificación de datos están surgiendo, pero aún no son de uso general”. (p. 14)

Y aunque la mayoría actualmente aún realiza el proceso de forma manual, existen mecanismos automatizados como el proyecto Apache Jackrabbit de la Fundación Apache.

Data Loss Prevention

Gartner (2017) define el mercado DLP como:

“Aquellas tecnologías que, como función central, proporcionan remediación para la pérdida de datos basándose tanto en la inspección del contenido como en el análisis contextual de los datos”. (p. 1)

Algunas de estas tecnologías se utilizan en datos que se encuentran en alguna de las condiciones o estados siguientes:

- En reposo en el local, o en aplicaciones y almacenamiento en la nube.
- En movimiento sobre la red.
- En uso en un dispositivo de punto final administrado.

Para Gartner (2017):

“Los productos DLP pueden ejecutar respuestas que van desde la simple notificación hasta el bloqueo activo basándose en políticas y reglas definidas para abordar el riesgo de fugas inadvertidas o accidentales o la exposición de datos sensibles fuera de los canales autorizados”. (p. 1)

Las tecnologías DLP se pueden dividir en dos categorías distintas:

- Los DLP empresariales: incorporan técnicas sofisticadas de detección para ayudar a las organizaciones a resolver sus requisitos más críticos de protección de datos. Los productos van desde software de agente para escritorios y servidores, dispositivos físicos y virtuales para monitorear redes y agentes, hasta dispositivos para el descubrimiento de datos.

  Las principales características de los productos DLP empresariales incluyen:

  - Una consola de administración centralizada.
  - Soporte para la definición de políticas avanzadas.
  - Flujo de trabajo de gestión de eventos.
  - Generación de informes.

  En resumen, un DLP empresarial funciona como un sistema completo para descubrir datos sensibles dentro de una organización y mitigar el riesgo de su pérdida en los puntos finales, en almacenamiento y en la red.

- Los DLP integrados: ofrecen funciones DLP limitadas que se integran en otros productos de seguridad, incluyendo, pero no limitado *gateways* web seguros (SWGs), *gateways* seguros de correo electrónico (SEGs), *firewalls* de red corporativos (ENFW), sistemas de detección y prevención de intrusiones. IDPS), productos de cifrado de correo electrónico, plataformas de gestión de contenido empresarial (ECM), herramientas de clasificación de datos, herramientas de descubrimiento de datos y agentes de seguridad de acceso a la nube (CASB).

En resumen, un DLP integrado por lo general se centra en el cumplimiento normativo y en casos básicos de uso de propiedad intelectual donde los datos

dirigidos a la protección son fácilmente identificables y la política de remediación es sencilla.

A continuación, se muestra una imagen con las tecnologías DLP por considerar para la prevención contra la pérdida de datos empresariales, según Gartner (2017).

Cuadrante mágico

Figura 1. Cuadrante mágico para la prevención contra la pérdida de datos empresariales

Fuente: Gartner (2017).

Por su parte, Symantec (2015) hace mención a que:

> *"Si se utiliza la configuración inicial de su servidor, su DLP no detecta ni notifica de la existencia de metadatos en documentos. Para que puedan ser detectados es necesario que se modifique la configuración y se habilite el valor "ContentExtraction.EnableMetaData" y de esta forma que se puedan detectar metadatos en documentos de Microsoft Office y en archivos PDF". (p. 1)*

A su vez, cabe considerar que, si se habilita la opción de detectar metadatos, esto podrían causar la aparición de falsos positivos en los resultados de las búsquedas.

Tagging

Es un mecanismo de etiquetado que permite organizar contenido y dar facilidades al realizar búsquedas en casos donde se da tratamiento a grandes volúmenes de información.

Existen actualmente herramientas que permiten realizar una clasificación de los datos de manera automática, reduciendo el esfuerzo que conllevaría realizar el proceso manualmente; por ejemplo, la herramienta de código abierto SCAN[5] (Smart Content Aggregation and Navigation) que administra contenido semántico personal y que puede combinar funciones de búsqueda, análisis de texto, etiquetado y metadatos para proporcionar una nueva experiencia de usuario de navegación de escritorio y gestión de documentos personales.

Como menciona Paz (2017):

> *"SCAN ofrece un rico conjunto de propiedades de metadatos asociados a los documentos, incluyendo: el título del documento, descripción, anotaciones, autor, fecha de creación y otros. Las propiedades se establecen automáticamente en el documento y se pueden añadir y editar*

[5] http://scan.sourceforge.net/

rápidamente después. Las propiedades de los metadatos se pueden utilizar en las consultas de búsqueda para encontrar los documentos que coincidan con los criterios especificados. Además, algunas propiedades (autor, trayectoria, fecha e idioma) sirven como tags de navegación para recorrer los documentos". (p. 1)

Cifrado de datos

Es un mecanismo que permite que una información legible se transforme mediante un algoritmo (cifra) en información ilegible (criptograma o secreto), de esta forma, que esta información se pueda enviar a un destinatario con menores posibilidades de que pueda ser conocida por terceros sin autorización.

A este proceso también se le conoce en idioma inglés como "encrypt".

Medidas de prevención y seguridad para la fuga de información

Es importante mencionar que mucha de la documentación que existe está en función de prevenir la fuga de información en general, no así la fuga de datos que se produce por metadatos, tal y como se muestra en las medidas de prevención y seguridad que recomienda INCIBE (2016):

"Las principales medidas de prevención deben orientarse hacia el componente humano y organizativo que se encuentra dentro de las causas de este tipo de incidentes. La prevención de la fuga de información pasa por la aplicación de medidas de seguridad desde tres puntos de vista: técnico, organizativo y legal.

Medidas Organizativas:

- *Poner en marcha buenas prácticas para la gestión de fuga de la información.*

- *Definir una política de seguridad y procedimientos para todo el ciclo de vida de los datos.*
- *Establecer un sistema de clasificación de la información, para ligarlo a roles y niveles de acceso.*
- *Llevar a cabo acciones de formación e información interna en ciberseguridad.*
- *Implantar un sistema de gestión de seguridad de la información.*

Medidas Técnicas:

- *Control de acceso e identidad.*
- *Soluciones anti-malware y anti-fraude, seguridad perimetral y protección de las telecomunicaciones.*
- *Control de contenidos, control de tráfico y copias de seguridad.*
- *Control de acceso a los recursos, actualizaciones de seguridad y parches.*

Medidas Legales:

- *Solicitud de aceptación de la política de seguridad y de la de conformidad por parte de los empleados.*
- *Medidas relativas a la adecuación y cumplimiento de la legislación aplicable (LOPD, LSSI, etc).*
- *Otras medidas de carácter disuasorio en base a la legislación.*

Cada organización es diferente y será necesario buscar un equilibrio entre complejidad, coste y riesgo, en relación con la implantación de las medidas de seguridad. Pero el asesoramiento profesional, no solo durante la gestión de un incidente de fuga de información, sino también, en la fase de diseño de las medidas de prevención es de vital importancia". (p. 18)

Y aunque sea importante contemplar todo tipo de medidas que permitan prevenir la fuga de datos, en lo que se refiere a metadatos no existen recomendaciones al respecto.

4.3.2 Estrategia 2:

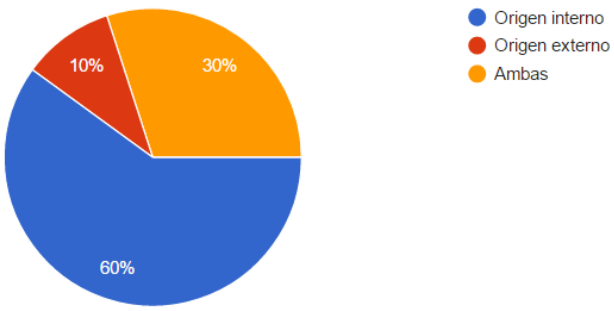
Importancia que se le da en las instituciones públicas de Costa Rica a la fuga de datos producida a través de metadatos.

Referente a la estrategia 2, se utiliza como instrumentos las entrevistas y el cuestionario, dirigidos a los profesionales de seguridad informática y personal de TI, con el fin de conocer la importancia que tienen para las instituciones públicas de Costa Rica la fuga de datos a través de metadatos.

Objetivo: Conocer la importancia que se le da en las instituciones públicas de Costa Rica a la fuga de datos producida a través de metadatos.

De los instrumentos aplicados se obtiene la siguiente información.

Figura 2. Motivador principal para que se dé una fuga de información

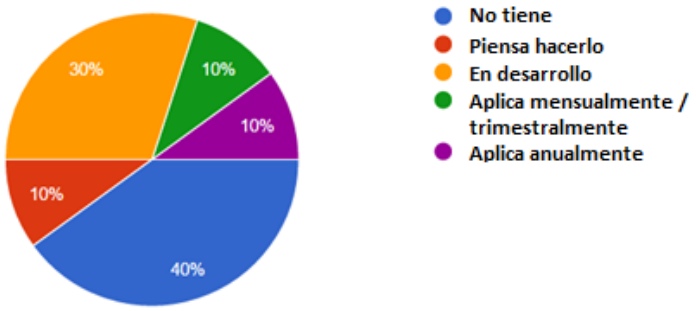


Fuente: Elaboración propia a partir del cuestionario aplicado a profesionales de seguridad informática y seguridad de la información (2017).

Análisis e interpretación

De la información recopilada y presentada anteriormente, se puede interpretar que la mayoría de los profesionales (60%) consideran que la fuga de datos tiene como principal motivador acciones internas de la institución, siendo necesario atender según el criterio profesional en un 30% situaciones internas y externas que podrían afectar la institución, mientras que un 10% considera el origen externo como único motivador de una fuga de información.

Figura 3.Políticas de educación a los usuarios respecto al uso de la información

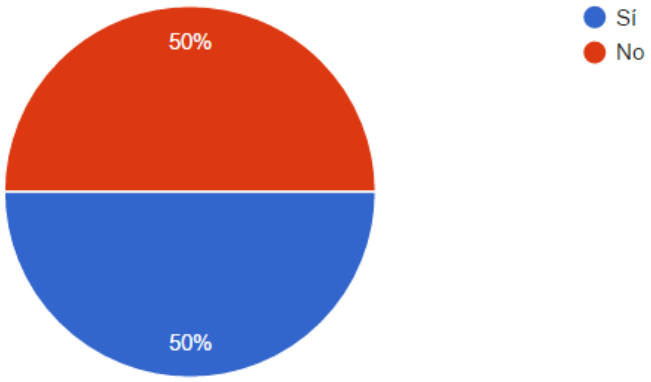


Fuente: Elaboración propia a partir del cuestionario aplicado a profesionales de seguridad informática y seguridad de la información (2017).

Análisis e interpretación

Referente a la figura 3, se puede determinar que un 80% de los encuestados afirma que la institución no cuenta con políticas de educación para el usuario respecto al uso correcto de la información, pues un 40% indica que no las tiene implementada, un 10% piensa construirlas, y un 30% indica que las está desarrollando. Se puede inferir de lo anterior que los usuarios de estas instituciones podrían no realizar un manejo adecuado de la información, siendo necesario a lo interno que se consideren acciones para mejorar este hecho.

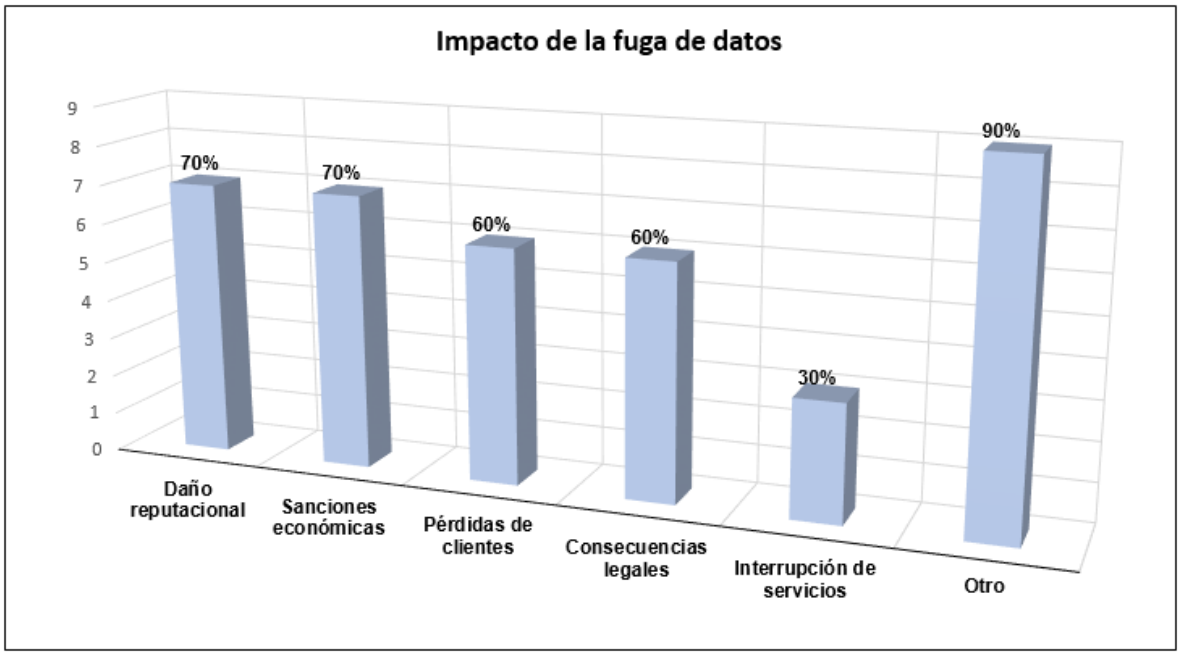
Figura 4. Se realizan procesos de evaluación de riesgo de pérdida de la información



Fuente: Elaboración propia a partir del cuestionario aplicado a profesionales de seguridad informática y seguridad de la información (2017).

Se consultó si se aplica en su organización procesos de evaluación de riesgo como mecanismo para atender el tema de pérdida de la información, además de si existe una asignación de privilegios según las necesidades que debería tener cada área y persona en la institución. Para ambas consultas los encuestados en porcentajes de 50% dividen opiniones en si se consideran o no adecuadamente los aspectos mencionados, mostrando con esto que un 50% no realiza este tipo de acciones para atender la pérdida de datos.

Figura 5. Impacto de la fuga de datos

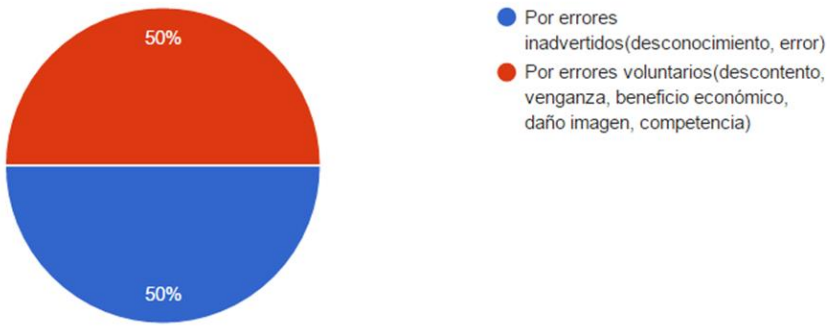


Fuente: Elaboración propia a partir del cuestionario aplicado a profesionales de seguridad informática y seguridad de la información (2017).

Con relación a cuáles serían los impactos más severos que tendría una fuga de datos, se consideran el daño reputacional y las sanciones económicas como los principales aspectos a tomar en cuenta, acaparando ambos la opinión del 70% de los encuestados, mientras que un 60% considera la pérdida de clientes y consecuenciales legales como los impactos más críticos de llegar a ocurrir una fuga de datos. Además, las interrupciones o fallas que limitan la continuidad de equipos/servicios no son contempladas por los encuestados como factores determinantes, ya que solo un 30% de ellos considera que pueden que pueden causar algún impacto para la institución y enfatizan que de presentarse una situación de este tipo debe atenderse, porque puede afectar la operación normal, pero no porque represente un factor que pueda potenciar una fuga de datos.

Esto permite inferir que el daño reputacional (pérdida de imagen, clientes) y las sanciones (legales, económicas) son las consecuencias más críticas que puede sufrir una institución si se evidencia la ocurrencia de una fuga de datos.

Figura 6. Motivos internos que podrían producir una fuga de datos.



Fuente: Elaboración propia a partir del cuestionario aplicado a profesionales de seguridad informática y seguridad de la información (2017).

De la información recopilada y mostrada en el gráfico anterior, se puede interpretar que a criterio de los encuestados resulta de igual importancia considerar como motivos internos que podrían producir una fuga de datos los errores voluntarios e involuntarios (inadvertidos), ambos representados por 50%.

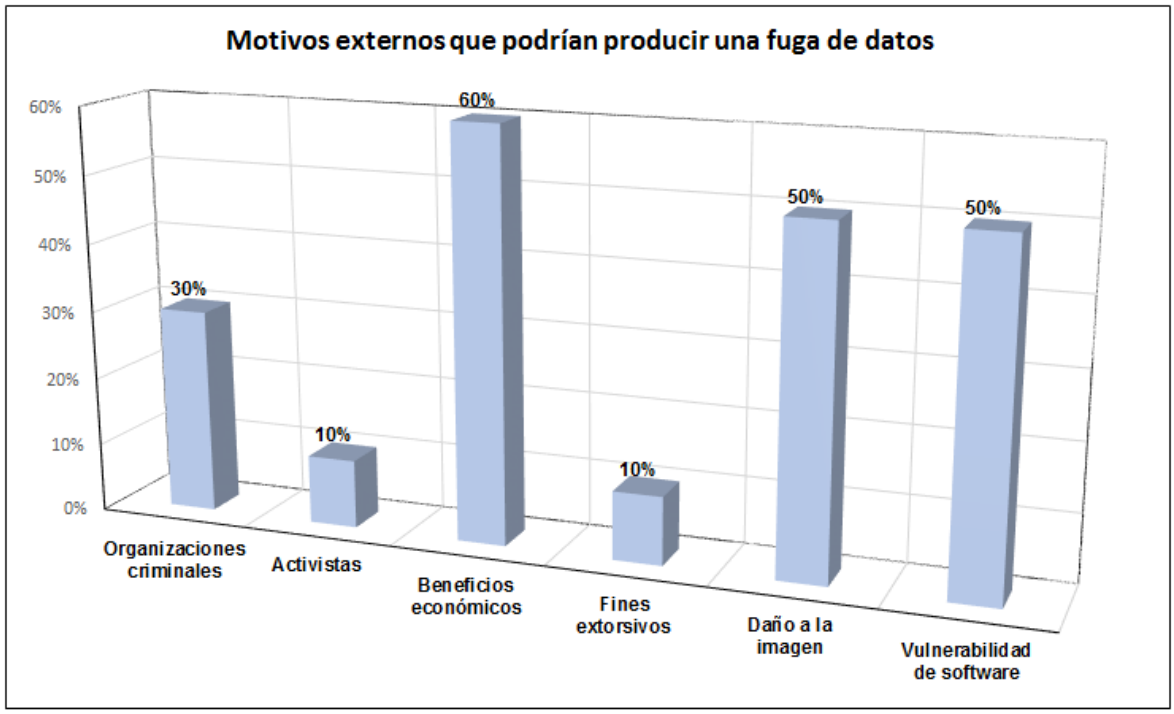
Relacionado a esta consulta realizada, es importante recalcar que para cada una de las categorías (errores voluntarios e involuntarios) los entrevistados mencionan un aspecto como el de principal importancia.

En el caso de errores inadvertidos, el 70% determinó que los causados por desconocimiento deberán tener prioritaria atención, aunado a que tienen la particularidad de que son más difíciles de mitigar, porque se desconoce “cuándo” o “cómo” podrían suceder, por lo que recomiendan importante enfatizar en aspectos como capacitar y concientizar al personal de la institución como una

medida preventiva para atender tales errores. En el caso de errores voluntarios, el 90% de los entrevistados indica que en donde medien beneficios económicos tendrán mayor cantidad de ocurrencia e impacto, pues al haber un incentivo se dedicaran mayores esfuerzos y recursos para tal fin.

Lo anterior deja en evidencia la importancia y lo necesario que resulta para las instituciones concientizar en prevenir la ocurrencia de estas situaciones, para que así se asignen los recursos necesarios que permitan que se atienda adecuadamente.

Figura 7. Motivos externos que podrían producir una fuga de datos.



Fuente: Elaboración propia a partir del cuestionario aplicado a profesionales de seguridad informática y seguridad de la información (2017).

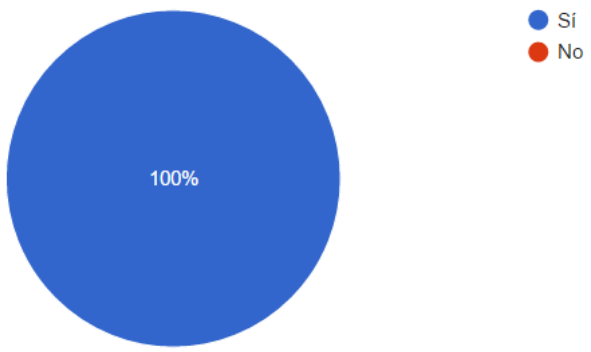
Enfatizando ahora en los aspectos externos, la figura anterior permite visualizar que el mayor porcentaje de los encuestados (60%) indica que el principal motivo externo que podría producir una fuga de datos en una institución

lo constituye el obtener beneficios económicos, mientras que un 50% considera el daño a la imagen y las vulnerabilidades que presenten los equipos en las instituciones como los posibles motivos. Con menos porcentaje (un 30%) se considera un aspecto que a nivel mundial se está desarrollando y que reviste de importancia a considerar como lo es las organizaciones criminales. Finalmente, con un poco menos de criticidad según los datos recopilados, se consideran motivos externos los fines activistas y extorsivos representados ambos por un 10% de los encuestados.

Metadatos

Aunando en el tema de metadatos se consulta si resulta familiar el concepto de metadatos, y si consideran que esta puede ser una causa de fuga de datos obteniendo al respecto la información que se muestra a continuación.

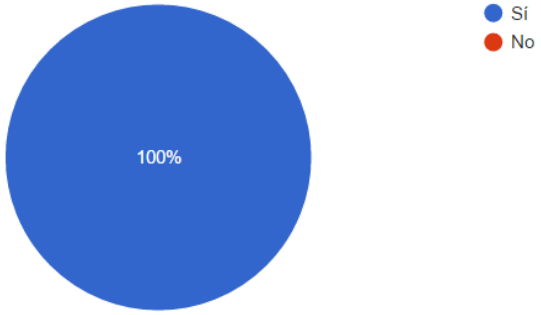
Figura 8. Los metadatos



Fuente: Elaboración propia a partir del cuestionario aplicado a profesionales de seguridad informática y seguridad de la información (2017).

El 100% de la muestra consultada afirma conocer qué son los metadatos (ver figura 8); también el 100% afirma que puede existir fuga de información a través de metadatos tal y como se ilustra en lafigura9.

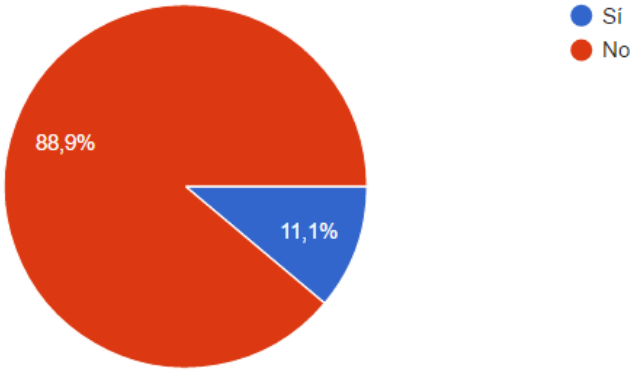
Figura 9. Fuga de información a través de metadatos



Fuente: Elaboración propia a partir del cuestionario aplicado a profesionales de seguridad informática y seguridad de la información (2017).

No obstante, aquí es donde se muestran aspectos que dejan en evidencia situaciones que no concuerdan y que se mostrarán y detallarán a continuación.

Figura 10. Limpieza de metadatos en documentos



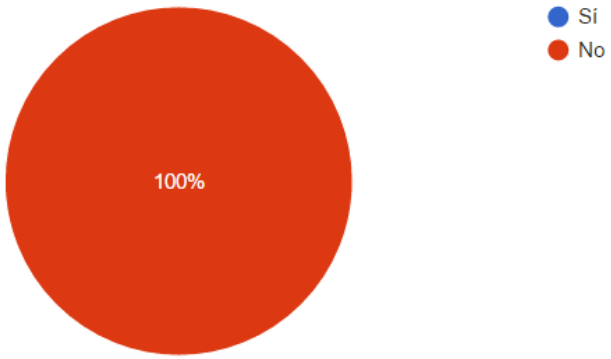
Fuente: Elaboración propia a partir del cuestionario aplicado a profesionales de seguridad informática y seguridad de la información (2017).

Aunque el 100% de los encuestados afirma conocer qué son los metadatos (ver gráfico N°8) y el mismo 100% (ver gráfico N°9) afirma saber que puede existir fuga de datos por medio de metadatos, solo el 11.1% de ellos alega realizar

esfuerzos para atender el tema de limpieza de metadatos a documentos de acceso público, dejando al restante 88.9% de las instituciones vulnerables y con una problemática que atender. Esto evidencia que a pesar de que existe algún tipo de conocimiento del tema, a lo interno de las instituciones muy poco o casi nada es lo que se realiza para atender esta situación. Así, se demuestra demostrando así que a pesar de realizar esfuerzos como inversiones de recursos económicos, profesionales, capacitaciones, procesos de concientización, entre otros, existen vulnerabilidades que amenazan a las instituciones y generan un riesgo, que debe principalmente darse a conocer y posterior a esto atenderse del mismo modo que otros escenarios en los que pueda existir fuga de información.

Como lo evidencia la figura N°11, la atención a este tipo de fuga de datos simplemente no se realiza.

Figura 11. Atender el tema de fuga de datos a través de metadatos

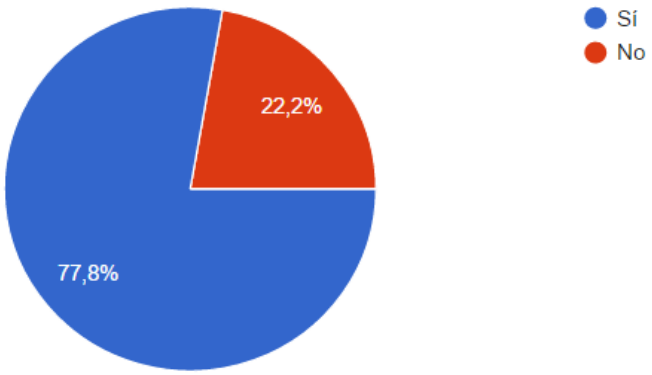


Fuente: Elaboración propia a partir del cuestionario aplicado a profesionales de seguridad informática y seguridad de la información (2017).

Según lo expuesto en el grafico anterior, se visualiza una brecha que puede ser utilizada por terceros para obtener información, esto porque no se atiende el tema de fuga de datos que se pueda producir por medio de metadatos contenidos en documentos de acceso público. A su vez, la problemática se incrementa, debido a que un 22% de los encuestados dice que no se atiende la fuga de datos

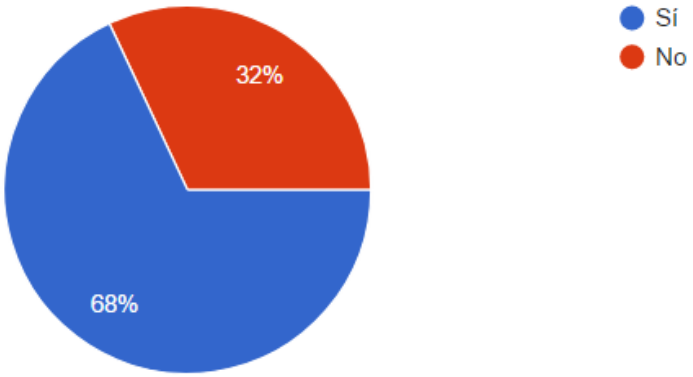
producida en las instituciones en las cuales labora, tal y como se visualiza en la figura 12:

Figura 12. Atiende el tema de fuga de datos



Fuente: Elaboración propia a partir del cuestionario aplicado a profesionales de seguridad informática y seguridad de la información (2016).

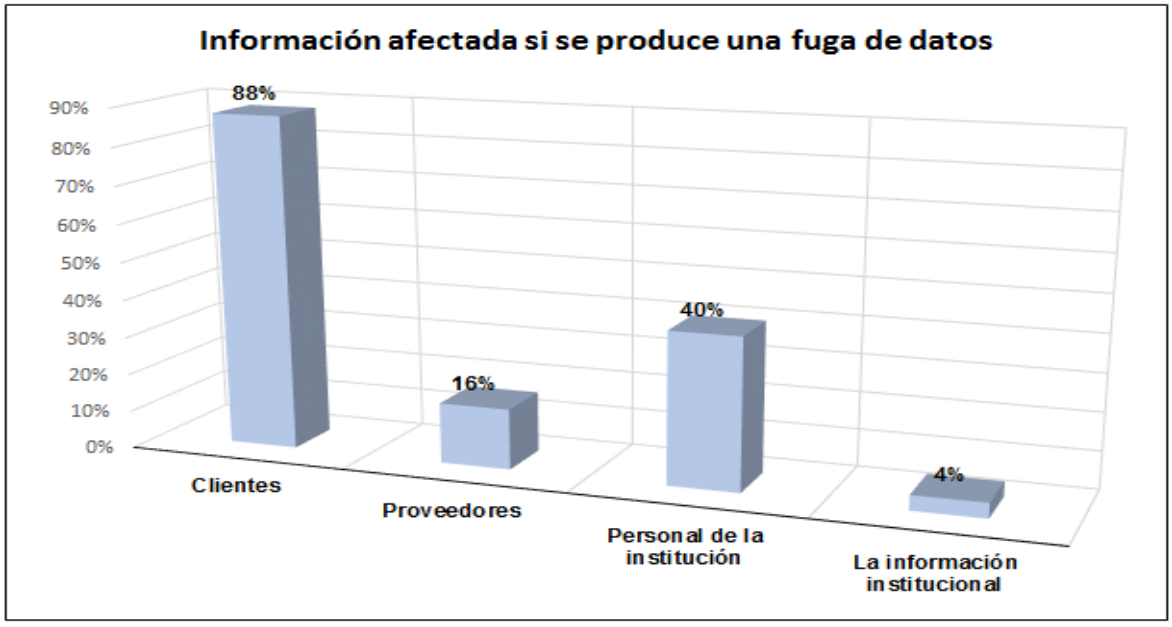
Figura 13. Políticas o lineamientos de seguridad para atender el tema de la fuga de datos



Fuente: Elaboración propia a partir del cuestionario aplicado a profesionales de seguridad informática y personal de TI(2016).

De la información recopilada y mostrada en el gráfico anterior (figura 13), es meritorio señalar que el 68% de los profesionales indicó que contaban con una política de seguridad o lineamientos internos para garantizar la seguridad y privacidad de la información interna y de sus usuarios, pero el restante 32% de ellos afirma que no es así. Lo anterior demuestra que este es un tema importante para las instituciones y que se están realizando esfuerzos para asegurar un adecuado tratamiento a la información. No obstante, y a pesar de lo trascendental que se considera el tema a nivel mundial en la actualidad, aun otras instituciones no lo atienden con la importancia que debe tener o no han buscado los mecanismos necesarios para prevenir y reducir los efectos negativos (legales, reputacionales, operativos) que pudiera causar la fuga de datos en una institución.

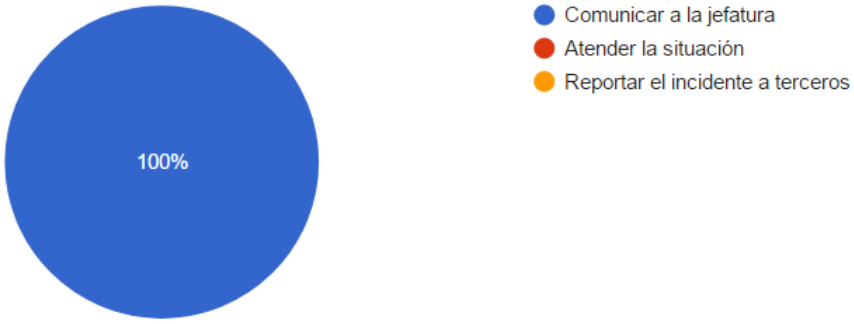
Figura 14. Información afectada si se produce una fuga de datos



Fuente: Elaboración propia a partir del cuestionario aplicado a profesionales de seguridad informática y personal de TI (2016).

En la figura anterior, los encuestados, representados por un 88%, consideran que, en caso de producirse una fuga de datos, la información de los clientes es la más afectada. Un grupo menor, correspondiente al 40%, expresa que la información del personal de la institución tendría una gran afectación; con un valor más bajo (16%), la información de los proveedores podría ser la afectada y un 4% considera otra información a lo interno de la institución como la que podría verse afectada. A raíz de lo anterior, se considera trascendental para cualquier entidad, que exista una clasificación de los datos, para posteriormente poder asignar los controles necesarios con el fin de protegerla y, de esta forma, minimizar el riesgo o evitar que una vulneración pueda ocasionar daños a sus intereses.

Figura 15. ¿Qué hacer en caso de detectar una fuga de información?



Fuente: Elaboración propia a partir del cuestionario aplicado a profesionales de seguridad informática y personal de TI (2016).

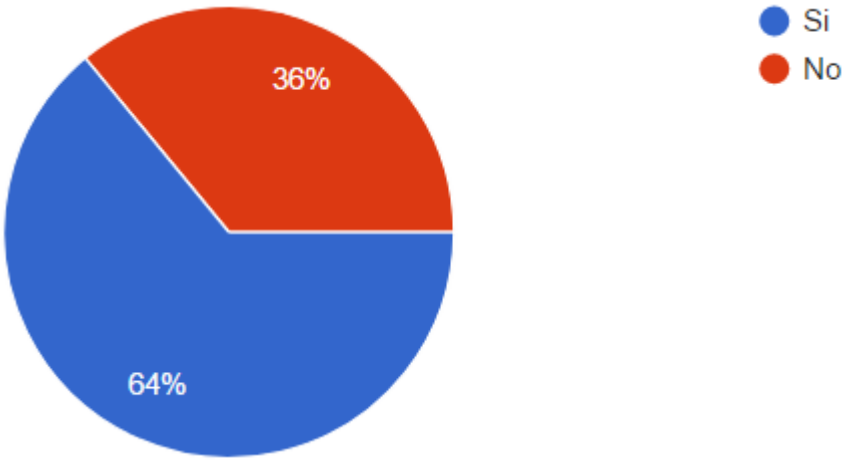
Ante lo anterior (figura 15), el 100% de los encuestados considera que, en caso de detectar una fuga de datos en la institución, se lo comunicaría a sus jefaturas.

Para que las consecuencias de una fuga de información sean mínimas, es fundamental que, ante cualquier situación sospechosa, se notifique al superior

inmediato o en su defecto al área de respuesta a incidentes, ya que serían quienes tomen las mejores decisiones para atender este tipo de incidentes. Una comunicación oportuna indudablemente minimizaría el impacto que pueda tener este tipo de situaciones.

De la mano con la existencia de políticas y lineamentos a lo interno de las instituciones existe un aspecto de principal trascendencia que debe considerarse y se basa en el hecho de que es igual de importante que se desarrolle una política o directriz, a que la conozca todo el personal de la entidad.

Figura 16. Conocimiento de políticas o lineamientos en toda la institución



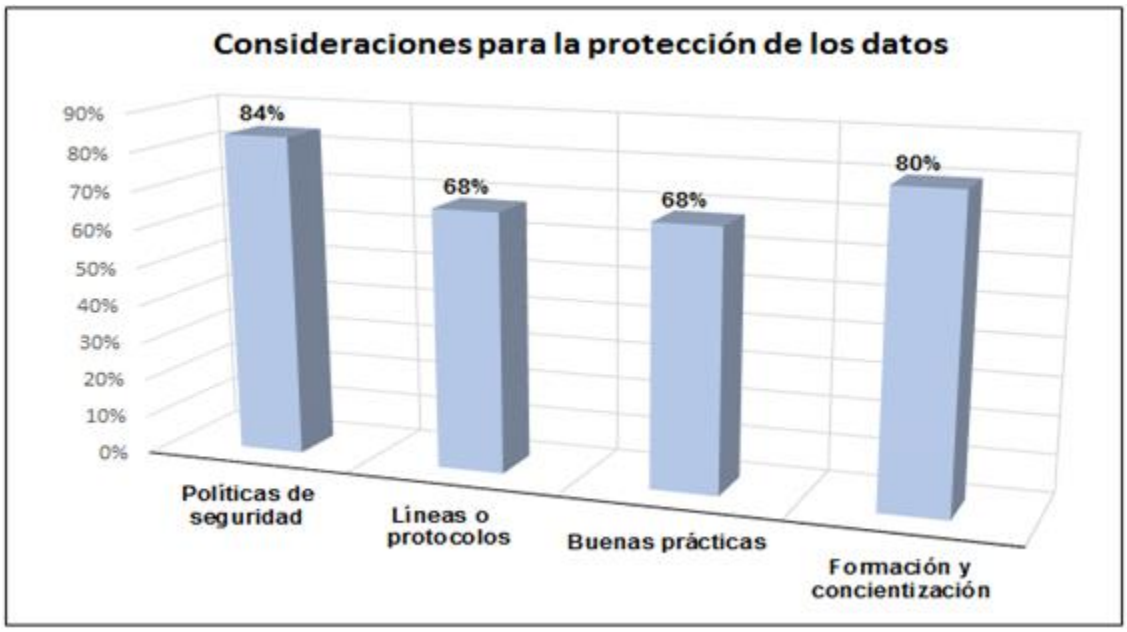
Fuente: Elaboración propia a partir del cuestionario aplicado a profesionales de seguridad informática y personal de TI (2016).

Como se aprecia en el anterior gráfico, existe un 36% que afirma que los documentos desarrollados y en los cuales se invierte muchos esfuerzos y recursos (humanos, financieros, entre otros.) no son de conocimiento de toda la institución, lo cual deja en evidencia problemas de comunicación que existen a lo interno de las instituciones.

Adicionalmente, se puede afirmar que los esfuerzos para divulgar son diversos y no responden a un objetivo coordinado, por lo cual este también es un tema que debe contemplarse y atenderse.

Es importante recalcar la importancia de desarrollar los lineamientos y las políticas que se deben seguir a lo interno de las instituciones, así como que se comuniquen asertivamente, pues de no ser así no se tendría un beneficio total de lo deseado y por lo que se han dedicado tantos esfuerzos y recursos en desarrollo. Además, un sector de la institución se convertiría en víctimas potenciales, que podrían ser vulnerables debido a su desconocimiento sobre el tema.

Figura 17. Acciones para la protección de los datos



Fuente: Elaboración propia a partir del cuestionario aplicado a profesionales de seguridad informática y personal de TI (2016).

Con referencia al gráfico 17, se puede interpretar que para los encuestados todos los aspectos son importantes. Primordialmente, considera un 84% de ellos que una política de seguridad es el mecanismo prioritario para atender a nivel institucional el tema de protección de datos. Así mismo, un 80% de ellos considera que la concientización y la formación profesional constituye un mecanismo trascendental por considerar. Además, para los aspectos de líneas base o

protocolos, y lo relacionado al seguimiento de buenas prácticas, el 68% de los encuestados en ambos casos considera la implementación de estos mecanismos como acciones que se deben seguir y desarrollar a nivel institucional.

4.3.3 Estrategia 3:

Normativa y legislación en materia de seguridad de la información que contribuyen en la prevención de la fuga de datos originada por metadatos contenidos en documentos de acceso público en Costa Rica.

Referente a la estrategia 3, se realizó una recopilación de normativa y legislación en materia de seguridad de la información que contribuye en la prevención de la fuga de datos.

Objetivo: Elaborar una recopilación de normativa y legislación en materia de seguridad de la información que contribuyen en la prevención de la fuga de datos originada por metadatos contenidos en documentos de acceso público en Costa Rica.

En el ámbito nacional, no existe normativa o legislación asociada al tema de fuga de datos originada por metadatos, pues la regulación existente básicamente se enfoca en la protección de datos personales.

- **Ley de Protección de la Persona frente al tratamiento de sus datos personales N° 8968**

Esta ley tiene como objetivo garantizar a cualquier persona, independientemente de su nacionalidad, residencia o domicilio, el respeto a sus derechos fundamentales, concretamente, su derecho a la autodeterminación informativa en relación con su vida o actividad privada y demás derechos de la

personalidad, así como la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes.

Además, indica que será de aplicación a los datos personales que figuren en bases de datos automatizadas o manuales, de organismos públicos o privados, y a toda modalidad de uso posterior de estos datos.

Se enfatiza como tal en el derecho fundamental a la autodeterminación informativa, con el objeto de controlar el flujo de informaciones que conciernen a cada persona, derivado del derecho a la privacidad, entre otros aspectos.

“Recuperado de la Agencia de Protección de Datos de los Habitantes de Costa Rica (PRODHAB) el miércoles 1 de marzo del 2017” de “http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=70975&nValor3=85989&strTipM=TC”

- **Reglamento a la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales N°37554-JP**

Las disposiciones de este documento tienen por objeto reglamentar la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales.

Un aspecto importante a considerar que se incluye en el Reglamento N°37554-JP corresponde al artículo 38, sobre vulnerabilidad de seguridad. Donde ahí se menciona que el responsable deberá informar al titular sobre cualquier irregularidad en el tratamiento o almacenamiento de sus datos, tales como pérdida, destrucción, extravío, entre otras, como consecuencia de una vulnerabilidad de la seguridad o que tuviere conocimiento del hecho, para lo cual tendrá cinco días hábiles a partir del momento en que ocurrió la vulnerabilidad, a fin de que los titulares de estos datos personales afectados puedan tomar las medidas correspondientes.

Y como se indica en el artículo 39, sobre información mínima, en caso de una vulneración a la seguridad se deberá informar al titular y a la agencia (PRODHAB), en un plazo no mayor a 5 días después de ocurrido o detectado esta situación.

“Recuperado de la Agencia de Protección de Datos de los Habitantes de Costa Rica (PRODHAB) el miércoles 1 de marzo del 2017” de “http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=74352&nValor3=106487&strTipM=TC”

- **Manual de buenas prácticas para el manejo de los datos personales de los clientes de los servicios financieros.**

Este manual busca promover y asesorar a las entidades financieras en el tema de protección de datos, protegiendo la autodeterminación informativa de sus clientes. Tiene como objetivo principal de su desarrollo que se puedan conocer los datos que tenga la entidad financiera respectiva; los fines para los cuales esos datos están destinados y que estos sean empleados solamente para el fin permitido por el ordenamiento jurídico; además, incluye como otro de los aspectos importantes en caso de que los datos sean incorrectos, o inexactos, o estén siendo utilizados para un fin distinto del cual legítimamente pueden cumplir, que sean rectificados, actualizados, complementados o suprimidos,.

Es importante considerar, según lo afirma el autor, que este documento es concordante con las disposiciones establecidas tanto por la legislación y normativa vigente emitida por los órganos reguladores aplicable a los bancos o instituciones financieras, incluyendo las siguientes:

- Ley Orgánica del Sistema Bancario Nacional.
- Ley Orgánica del Banco Central de Costa Rica.

- Ley 5044 (de empresas financieras).
- Ley General de Administración Pública.
- Ley 8204 sobre Estupefacientes, Sustancias Psicotrópicas, Drogas de uso no Autorizado, Actividades Conexas, Legitimación de Capitales y Financiamiento al Terrorismo y su Normativa Conexa.
- Reglamento a la Ley 8204.
- Normativa Acuerdo SUGEF 12-10.
- Ley de Protección de la Persona frente al tratamiento de sus datos personales y su Reglamento.
- Reglamento de tarjetas de crédito y débito.
- Acuerdo SUGEF 7-06 denominado “Reglamento del Centro de Información Crediticia”.
- Acuerdo SUGEF 14-09 “Reglamento sobre la Gestión de la tecnología de la información”.

“Recuperado de Cámara de Bancos de Costa Rica el martes 7 de marzo del 2017” de “http://camaradebancos.fi.cr//wp-content/uploads/2015/07/Manual-de-buenas-pr%C3%A1cticas-para-la-aplicaci%C3%B3n-de-la-ley-de-protecci%C3%B3n-de-la-persona-frente-al-tratamiento-de-sus-datos-personales1.pdf”

En el ámbito internacional, el panorama es similar, la normativa o legislación existente es limitada, y las instituciones que tratan de atender la prevención de fuga de datos, lo realizan a nivel general, describiendo mayoritariamente usos y capacidades de tecnologías desarrolladas, en la protección de datos personales, pero no enfocadas directamente a la prevención

de fuga de datos que se origina por metadatos (en la mayoría de los casos ni se contempla)

- **¿Cómo gestionar una fuga de información?**

El documento, hace referencia a diversas interrogantes:¿Cómo podemos mitigar la fuga de información? ¿Qué debemos hacer si se produce una fuga de información en nuestra empresa?, sin embargo, lo hace desde la premisa de que la fuga de información tiene un componente social y humano muy importante y que detrás de muchos de estos incidentes se esconden motivaciones personales, económicas, daño a la imagen de la organización o simples errores, entre otras. También expone los factores que motivan y originan la fuga de datos, describiendo además las causas, las consecuencias y el impacto que puede tener una fuga de datos, así como los mecanismos de prevención que se pueden seguir. Su aporte principal es la presentación de un plan para la gestión de los incidentes de fuga de información en donde clasifica en fases su atención, describiendo aspectos que se deben considerar en cada una de las etapas.

“Recuperado del Instituto Nacional de ciberseguridad de España S.A. el miércoles 1 de marzo del 2017” de “https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_gestion_fuga_informacion_0.pdf”

- **Prevención de pérdida de datos (Data LossPrevention)**

El documento presenta una descripción de múltiples aspectos a considerar que debe tener una institución para elegir DLP (*Data Loss Prevention*). Muestra la importancia que tiene esta herramienta en la prevención de la pérdida de datos, pero sin olvidar que es solo una herramienta que puede contribuir, pero necesita de otros factores (personas, recursos, políticas, entre otros) para que sus resultados sean los esperados. Describe también que los puntos de salida comunes de este tipo de infracción de datos son correo electrónico corporativo,

correo web, FTP, unidades extraíbles e impresión, y que muchos de estos podrían prevenirse con la utilización de un DLP.

Además, manifiesta que las soluciones de DLP pueden funcionar para escenarios con datos en movimiento, en reposo y en puntos finales, teniendo para todos estos entornos elementos que pueden mejorar la seguridad y evitar que se dé una fuga de datos. Sin embargo, recalca la importancia de una adecuada elección de un proveedor de DLP, debido a la variedad de elementos y criterios de evaluación (seguimiento y prevención, gestión centralizada, requisitos de copia de seguridad y almacenamiento, facilidad de integración, presencia en el mercado, personal adicional) según las necesidades del negocio que podrían determinar esa elección, sin olvidar también el propósito por el que se quiere adquirir.

Por último, destaca que una solución de proveedor posiblemente viene acompañada de un precio elevado, pero que existen alternativas de soluciones gratuitas (snort, suricata, ipchains), las cuales han crecido y madurado y que podrían ser una opción por considerar como herramienta para la prevención de la pérdida de datos en una institución.

“Recuperado del Sitio Web de SANS Institute el martes 7 de marzo del 2017” de “https://www.sans.org/reading-room/whitepapers/dlp/data-loss-prevention-32883”

- **Recomendaciones para una metodología para la evaluación de la severidad de brechas en datos personales (Recommendations for a methodology of the assessment of severity of personal data breaches, ENISA).**

La Agencia de Seguridad de la Red e Información de la Unión Europea (ENISA) revisó las medidas existentes y los procedimientos en los Estados miembros de la UE con respecto a las infracciones de datos personales y publicó en 2011 un estudio sobre la aplicación técnica del art. 4 de la Directiva sobre

privacidad electrónica, que incluía recomendaciones sobre cómo planificar y preparar las brechas de datos, cómo detectarlas y evaluarlas, cómo notificar a las personas y las autoridades competentes y cómo responder a las violaciones de datos. También se incluyó una propuesta de metodología para la evaluación de la gravedad de infracciones de datos personales como anexo a las recomendaciones mencionadas, que no se consideró suficientemente madura como para ser utilizada a nivel nacional por las diferentes autoridades de protección de datos.

En este contexto, las Autoridades de Protección de Datos de Grecia y Alemania, en colaboración con ENISA, elaboraron una metodología actualizada para la evaluación de la gravedad de la violación de datos que podría ser utilizada tanto por los DPA como por los responsables del tratamiento de datos.

Los elementos centrales que deben tenerse en cuenta al evaluar esta gravedad son:

- Contexto de procesamiento de datos - tipo de datos violados ajustados al contexto en el que se utilizan.
- Facilidad de identificación del individuo con base en los datos violados.
- Circunstancias del incumplimiento que influyen adicionalmente en la gravedad de un incumplimiento La metodología presentada en este estudio se basa en un enfoque tan objetivo como sea posible sin dejar de ser lo suficientemente flexible como para ser adoptada por diferentes autoridades de protección de datos ajustándola a su tamaño, al sistema jurídico nacional y a otros factores. De acuerdo con diferentes requisitos, la puntuación de algunas categorías puede ajustarse para producir los resultados más apropiados.

Además, esta metodología ha sido diseñada con los siguientes objetivos:

- Proporcionar a los responsables de los datos una herramienta cuantitativa (en la medida de lo posible) para evaluar la gravedad de las

infracciones de datos y, en consecuencia, notificar a las autoridades competentes, así como a las personas afectadas. La herramienta también podría servir como un medio para que los controladores de datos determinen rápidamente las medidas de mitigación necesarias.

- Proporcionar a las autoridades nacionales competentes una herramienta para evaluar la gravedad de las infracciones notificadas por los responsables del tratamiento de datos.

- Apoyar a las autoridades nacionales competentes en el proceso de realización de análisis detallados y estadísticas sobre las violaciones comunicadas de datos personales.

- Contribuir a la armonización de la evaluación de la gravedad de las infracciones de datos personales en la Unión Europea, proponiendo una metodología común y la puntuación de la gravedad. Esto sería especialmente importante en el caso de las infracciones transfronterizas.

Recuperado de “https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/dbn-severity/at_download/fullReport”

- **Pilares de protección empresarial: Prevención de pérdida de datos (Pillars of Enterprise Protection: Data LossPrevention)**

Este artículo presenta aspectos generales de la fuga de datos, basándose en estadísticas para presentar cuáles causas son las más comunes para que se dé este tipo de incidentes, enfatizando en tecnologías de prevención y en desarrollo de políticas que permitan resguardar los tres contextos denominados como los más importantes: datos en reposo, en uso y en tránsito (movimiento). Además, enfatizan en la necesidad de crear procesos para la utilización de esta

tecnología, monitorearla para ver los resultados que muestra, configurarle opciones de protección que detecten comportamientos no autorizados, pero además administrarlas adecuadamente sería fundamental para obtener los mejores resultados.

El autor, además, enfatiza en que ninguna tecnología trabaja de manera efectiva de forma aislada y que necesita de un enfoque coordinado (persona y tecnología) para poder lograr los resultados esperados, que son tan importantes. Incluye las normas y los marcos de trabajo para establecer lo que hay que hacer, así como la evaluación de necesidades en una organización y, por supuesto la tecnología para proteger lo que se ha identificado que se necesita.

“Recuperado del Sitio Web de Corporación Symantec el martes 7 de marzo del 2017” de “https://www.symantec.com/content/en/us/enterprise/white_papers/b-dlp_protecting_info_WP_21032641.en-us.pdf”

- **Etiquetar datos para prevenir la fuga de datos: formar depósitos de contenido (Tagging Data to Prevent Data Leakage: Forming Content Repositories)**

Este documento expone la necesidad de que exista un mecanismo de control centralizado (CMS) que pueda determinar cómo, dónde y cuándo se comparte la información de una persona o grupo a otra. Para ello, propone un sistema de gestión de contenidos que se convierte en el portal en donde se registren todos los dispositivos a través de los cuales se trasladan datos de una estación de trabajo a otra, comenzando desde un área o departamento hasta una empresa entera.

Argumentan que ante la cantidad de datos que se producen en un solo día y la necesidad de utilizar nuevos mecanismos de intercambio, como Facebook, Google Plus, Twitter, WhatsApp, ente otros, el monitoreo de estos datos ya no es efectivo, ni es sostenible, si se utilizan soluciones antiguas, por lo cual enfatizan

en la necesidad de tener un sistema centralizado en donde los datos puedan ser etiquetados para evitar fugas de datos y, de esta forma, solo puedan compartirse y distribuirse a los empleados con derechos y privilegios previamente designados.

Al finalizar, exponen beneficios de obligar a los empleados a compartir y distribuir información a través del CMS y un *Data LossPrevention DLP.*

“Recuperado del Sitio Web de SANS Institute el martes 7 de marzo del 2017” de “https://www.sans.org/reading-room/whitepapers/dlp/tagging-data-prevent-data-leakage-forming-content-repositories-36967”

- CISM- ISACA

ISACA, en el libro oficial utilizado para preparar la **Certificación en Gestión de Seguridad de la Información** (Certified Information Security Manager, CISM), define la fuga de datos como la “Extracción o fuga de información mediante el vaciado de archivos de computadora o el robo de informes y grabaciones de computadoras”. (2015, p. 289)

Además, expone el concepto de fuga de datos asociado a una amenaza interna, la cual puede ser originada como parte de la interconexión dinámica denominada “factores humanos” que forma parte del modelo de negocios para la seguridad de la información. Este se compone de cuatro elementos (diseño de la estrategia de la organización, tecnología, personas y procesos) y puede verse afectado por cambios en las interconexiones y comportamientos, ya sea para romper el equilibrio o para estabilizar el modelo de seguridad.

Para atender esta situación, ISACA 2015 recomienda “que todos los recursos humanos de la empresa reciban capacitación sobre las habilidades pertinentes” (p. 43), y así evitar que algún factor humano afecte la estabilidad del modelo.

Además, se menciona que un gerente de seguridad de la información debe estar familiarizado con recursos tecnológicos (*firewall*, sistemas antivirus), pero enfatiza la importancia de conocer una metodología de prevención de fuga de datos (seguridad en medios extraíbles, filtrado de contenido, entre otros.) y tecnologías asociadas, con la finalidad de administrar con éxito un programa de seguridad de la información. Por ejemplo, deberá cuestionarse si a nivel de seguridad técnica, ¿están vigentes los procesos de desactivación correctos para evitar la fuga de datos?, entre otros aspectos.

- **Otras regulaciones**

Otras regulaciones que existen para promover y proteger la información sensible se mencionan a continuación:

- La Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA) que entre otras cosas disuade el fraude y el abuso de la información existente en la industria de la salud.
- El estándar de seguridad de datos utilizado en la industria de tarjetas de pago (PCI-DSS) que busca mejorar la confianza por quienes realizan diariamente transacciones financieras.

4.3.4 Estrategia 4:

Causas de la fuga de datos en las instituciones públicas de Costa Rica.

Referente a la estrategia 4, se utiliza como instrumento el análisis bibliográfico y el juicio de profesionales expertos en seguridad de la información que atienden el tema de fuga de datos, a su vez, el cuestionario y las entrevistas

dirigidos a los profesionales de seguridad informática y personal de TI son otros de los instrumentos utilizados.

Objetivo: Analizar las principales causas de la fuga de datos en las instituciones públicas de Costa Rica.

Causas de la fuga de datos

Existen algunos aspectos que se consideran como los principales potenciadores de que ocurra una fuga de datos en las instituciones y que a continuación de describen:

a- **El error humano:** estos a su vez pueden generarse por diversos aspectos que se consideran a continuación:

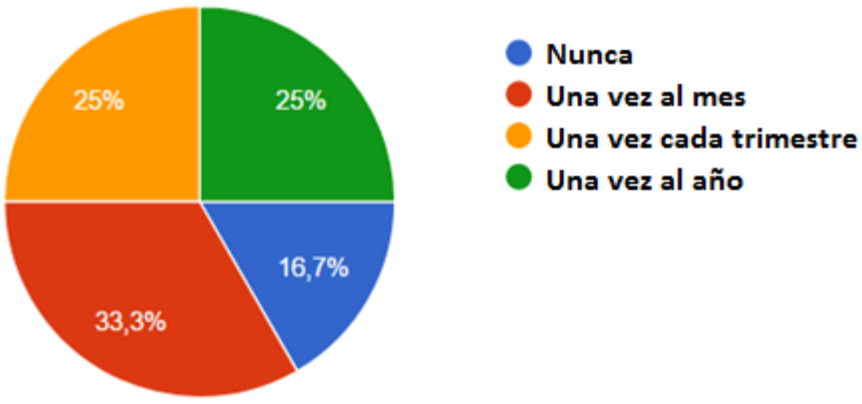
- **Situaciones voluntarias o involuntarias:** estas son la causa de muchas situaciones o incidentes de fuga de datos en las instituciones. Y es que como lo demuestra la empresa PWC en un estudio realizado en 2015, el 50 % de las brechas de mayor impacto fueron causadas de forma inadvertida. Esto demuestra que las amenazas internas que posteriormente propician fugas de datos no siempre deben asumirse como conductas maliciosas de las personas. Al respecto, WelivesSecurity (2016) describe que un ex empleado de una entidad en Estados Unidos se fue con una USB que contenía informes de 44 mil clientes, pero luego se demostró que dicho suceso fue completamente circunstancial.

  Y como se mostró anteriormente (ver gráfico N°5), los encuestados tienen una opinión dividida, pues consideran que en las mismas proporciones (representadas por un 50%) que por ambos factores podrían ocurrir incidentes debido a fugas de datos.
- **Ingeniería social:** forman parte de este grupo situaciones en donde personas, valiéndose de sus capacidades y habilidades en el manejo de situaciones y espacios, engañan a sus víctimas, logrando así obtener información que no debería ser de su conocimiento.

- **Gestión de la seguridad:** Otro aspecto de vital importancia lo constituye las malas (inadecuadas) decisiones en la gestión de la seguridad, y es que situaciones en las que la toma de decisiones no se realicen de la forma adecuada pueden impactar y acarrear que los profesionales a cargo no contemplen todos los escenarios y vectores que podrían dar lugar a fugas de datos.

Tal y como se muestra existen situaciones que evidencian debilidades en la administración de sus recursos. Todavía hay instituciones en las que según el criterio de los encuestados un 25% de ellos indica que por falta de recursos (económicos, humanos, técnicos) el software instalado se supervisa una vez al año, pero la situación se agrava, pues más de un 16% menciona que nunca se supervisan las aplicaciones instaladas en sus equipos de cómputo (ver figura 18).

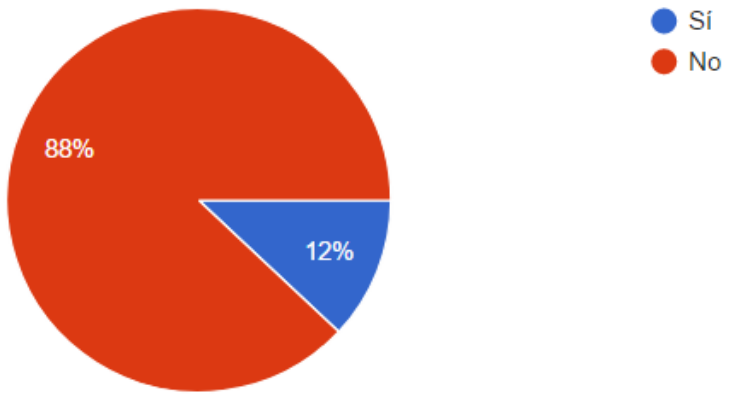
Figura 18. Supervisión de las aplicaciones (software) instaladas



Fuente: Elaboración propia a partir del cuestionario aplicado a profesionales de seguridad informática y seguridad de la información (2016).

Cabe analizar, a su vez, la siguiente figura:

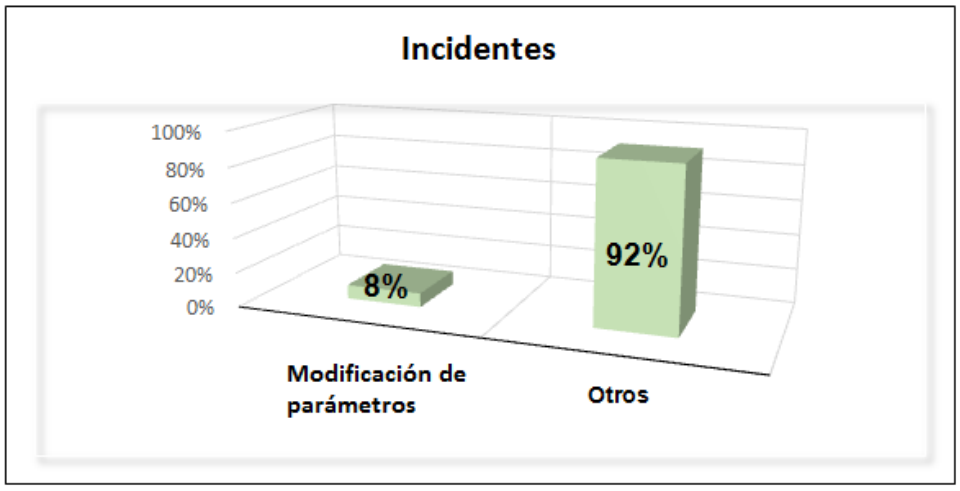
Figura 19. Modificación de parámetros y ajustes de seguridad



Fuente: Elaboración propia a partir del cuestionario aplicado a profesionales de seguridad informática y seguridad de la información (2016).

Así, para un 12% de los encuestados todavía se permite que los usuarios modifiquen parámetros y realicen ajustes que afecten la seguridad en los equipos que utilizan. Esto repercute directamente en situaciones de riesgo y amenazas para la institución, tal y como lo evidencia la figura N°20 que a continuación se presenta.

Figura 20. Incidentes de fuga de datos por la modificación de parámetros y ajustes de seguridad



Fuente: Elaboración propia a partir del cuestionario aplicado a profesionales de seguridad informática y seguridad de la información (2016).

Aquí se visualiza que un 8% de los incidentes que se detectan en las instituciones, corresponden a situaciones en las cuales se evidencia que personas (sin autorización, por debilidad de implementaciones, entre otras.) modifican parámetros y ajustes de seguridad, la cual repercute directamente en la seguridad de los usuarios finales, y acarreando consecuencias para la institución que la perjudica notablemente.

- **La educación y la formación:** constituyen un elemento trascendental en el manejo de situaciones de riesgo, en los procesos de toma de decisiones y en la culturización a lo interno de la entidad.

Resulta tan importante un dispositivo o una herramienta tecnológica que atienda este tipo de incidentes, como tener una adecuada formación en los profesionales y el personal a lo interno de la institución.

Es de vital importancia que durante cada proceso de concientización y de arraigo de hábitos en seguridad estos sean reforzados constantemente en el personal de la institución, porque de esta forma la responsabilidad de la protección de cualesquiera de los entornos institucionales no solo se delega en los profesionales de seguridad y en los personeros de tecnologías, sino que se convertirá en una labor colaborativa de todos en la organización, eso sí, con roles y responsabilidades claramente definidos y comunicados, en donde no haya duda de la labor que debe realizar cada uno.

Como se evidenció en la figura N° 3. *Políticas de educación a los usuarios respecto al uso de la información*, la existencia y el desarrollo de procesos de concientización o formación en las instituciones no son prioridad.

Y es que, según los datos recopilados, del total de los encuestados, un 40% indica que la institución no cuenta con tales políticas, un 10%

menciona que piensa hacerlas y un 30% dice que están en desarrollo. Esto permite discernir, si sumáramos los porcentajes anteriores, que un 80% de las instituciones no cuenta actualmente con procesos de educación y formación permanentes que permitan atender global e integralmente problemáticas que se presenten a lo interno de las instituciones.

Por esta razón, surge el cuestionamiento de ¿cómo se podría prevenir y/o atender una situación si no se conoce? Se visualiza con esto que se está descuidando quizás el principal aspecto necesario para atender una problemática, como es conocerla, pero para la gran mayoría de las instituciones al menos por ahora esto no es importante.

Ante este escenario, es fundamental trabajar para prevenir y evitar la ocurrencia tales de situaciones, que son causadas directa o indirectamente por personas a lo interno de la organización, y qué mejor manera para atender una situación que conociéndola y culturizando a quienes son parte de las instituciones.

b- **Robo:** es sin duda un riesgo que está presente en casi todos los entornos de una institución y del que no se escapan los datos. Por ello, el hecho de considerar desde protección física, hasta mecanismos como una adecuada segregación de funciones, una correcta asignación de roles, permisos (privilegios) establecidos correctamente y procesos de rotación de personal podrían prevenir la ocurrencia de estos.

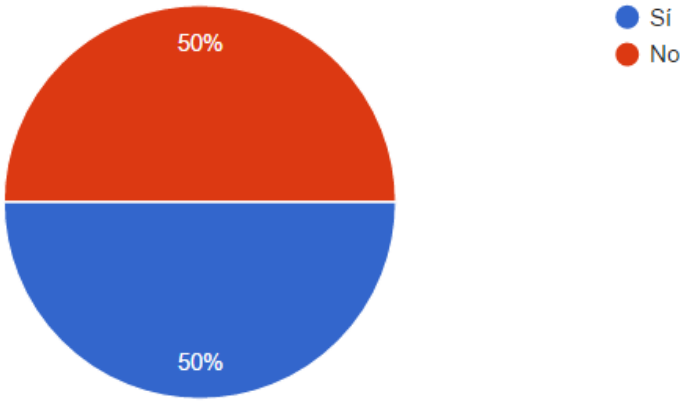
c- **Acceso no autorizado:** es común pensar que, para prevenir situaciones como la fuga de datos, son necesarios los controles de acceso robustos, el endurecimiento (*hardening*) de software, instalaciones, equipos, dispositivos, redes, pero también es necesario que quienes sí están autorizados para acceder a espacios físicos, a sistemas y a bases de datos lo realicen adecuadamente.

Los procedimientos y controles de seguridad pueden limitar este tipo de situaciones, pero deben ser complementados con decisiones correctas y una buena gestión. Así, según el reporte de la empresa Cisco en 2014:

> *"Un cuarto de los empleados admitió haber compartido información sensible con amigos, familiares o hasta incluso con extraños, pero además casi la mitad de los encuestados compartió dispositivos de trabajo con personas externas a la institución sin supervisión alguna." (p. 3)*

Esto demuestra que, por sí solos, los controles de seguridad no funcionan; necesitan de las personas y sus habilidades para una debida administración, siendo necesario, además, que este personal sea muy responsable en la labor que desempeña. Tal idea se ve reforzada con la consulta que se realizó y en la cual se preguntó si el acceso a la información en la entidad está acorde con los privilegios y necesidades que debería tener cada área y persona en la entidad. Como lo muestra el gráfico 21:

Figura 21. Asignación de roles y privilegios en las instituciones



Fuente: Elaboración propia a partir del cuestionario aplicado a profesionales de seguridad informática y seguridad de la información (2016).

Para la mitad de los encuestados (representados por el 50%), los privilegios con los que se cuenta a lo interno de las instituciones potencian el

que puedan ocurrir fugas de datos. Además, se indica en muchos casos que los usuarios desconocen que tienen algunos privilegios y, por tanto, no están conscientes del peligro y los riesgos que podrían generarse.

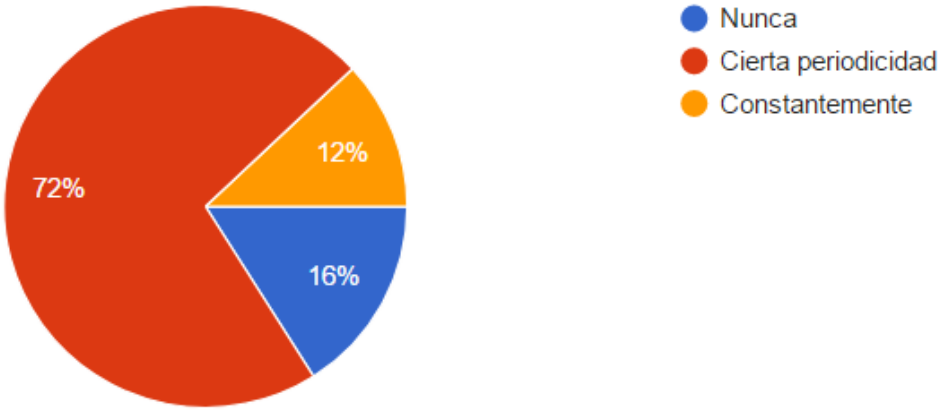
Es aquí donde aspectos como *mínima superficie de exposición* y *menor privilegio posible* son de vital importancia para ser considerados, del mismo modo que una *adecuada gestión en la asignación de perfiles y roles* dentro de las instituciones.

A su vez, de los aspectos citados, para INCIBE (2017) la información abandona la empresa por las siguientes formas:

> *"Mediante portátiles, móviles y otros dispositivos externos como discos duros, CD/DVD o USB que se extravían o se usan para «sacar» información. Se agrava si no se tiene control sobre los dispositivos permitidos (incluidos BYOD) y sobre la información que se puede copiar en ellos. Mejora si se controla qué información puede copiarse a estos dispositivos y en qué casos debe ir cifrada."(p. 1)*

La utilización de dispositivos móviles en la actualidad es una situación riesgosa que enfrentan las instituciones, siendo cada vez más común la utilización de estos sin algún tipo de control o regulación, aun cuando no se permitan. Y es que como se visualiza en el siguiente gráfico:

Figura 222. Utilización de equipos de cómputo institucionales para propósitos personales



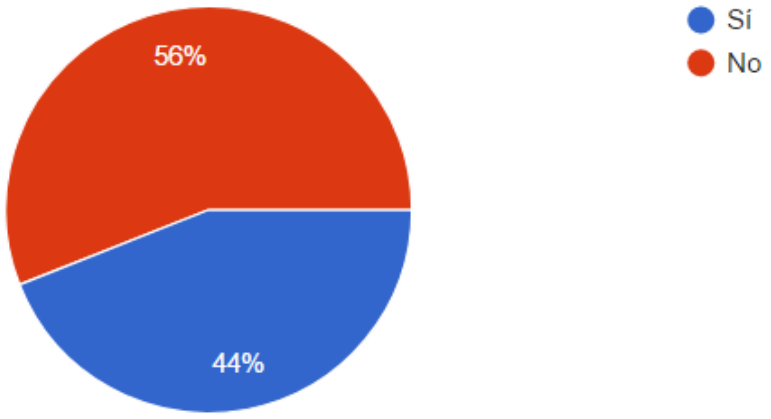
Fuente: Elaboración propia a partir del cuestionario aplicado a profesionales de seguridad informática y seguridad de la información (2016).

El 72% admite utilizar los dispositivos institucionales para propósitos personales con cierta periodicidad, un 12% indica que los utiliza constantemente y solo un 16% menciona que nunca los ha utilizado con otros propósitos que no sean los que se le asignaron como parte de su entorno laboral.

Esto demuestra la falta o inexistencia de controles que limiten e impidan su empleo para otros propósitos, pero además el que se estén generando nuevas fuentes de riesgo y de explotación que puedan afectar a las instituciones.

La situación no queda solamente ahí. Ante el siguiente cuestionamiento: ¿Transfiere o ha transferido información (datos) de un dispositivo de trabajo a un dispositivo personal?, un 44% de los entrevistados admite haber utilizado dispositivos personales para propósitos de trabajo tal y como se muestra a continuación en la figura 23.

Figura 233. Uso de dispositivos personales

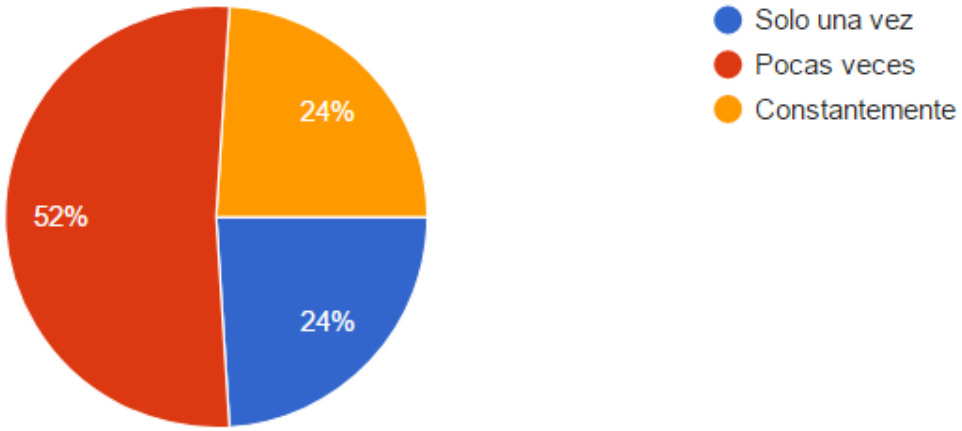


Fuente: Elaboración propia a partir del cuestionario aplicado a profesionales de seguridad informática y seguridad de la información (2016).

Pero, la problemática no termina ahí, pues la frecuencia con que se utilizan dispositivos personales en ambientes de trabajo en situaciones como el almacenamiento de la información es alarmante.

Según el siguiente gráfico:

Figura 244. Frecuencia de uso de dispositivos personales

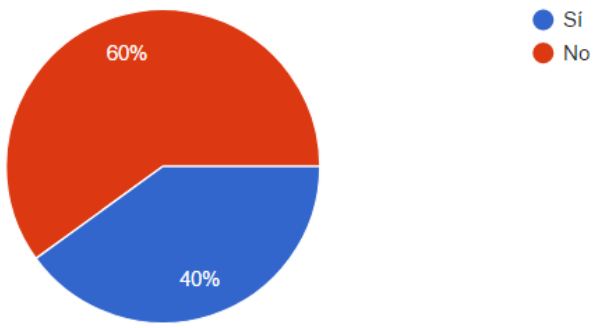


Fuente: Elaboración propia a partir del cuestionario aplicado a profesionales de seguridad informática y seguridad de la información (2016).

La recurrencia del uso de estos dispositivos es parte del día a día en las instituciones, y como se deduce de la figura N°24 el 100% del personal encuestado y entrevistado admite por lo menos una vez haber utilizado dispositivos personales para propósitos laborales, pero además y, como lo menciona la población consultada, muchas veces recurren al uso de estos dispositivos, porque en las instituciones no se cuenta con suficientes recursos; otras veces por facilidad, ya que se evitan papeleos y trámites para el traslado y uso de los recursos instituciones, pero muchos otros admiten que lo hacen hasta por desconocimiento de los riesgos asociados que puedan acarrear este tipo de acciones.

Esto demuestra que situaciones como las anteriormente descritas no solo son comunes, sino que representan una gran amenaza para las instituciones, las cuales en muchos de los casos se realizan por negligencia, desconocimiento y hasta porque no existen regulaciones que limiten su utilización, como se logra evidenciar en la figura 25:

Figura 255. Existe regulación para la utilización de dispositivos móviles personales en la institución.



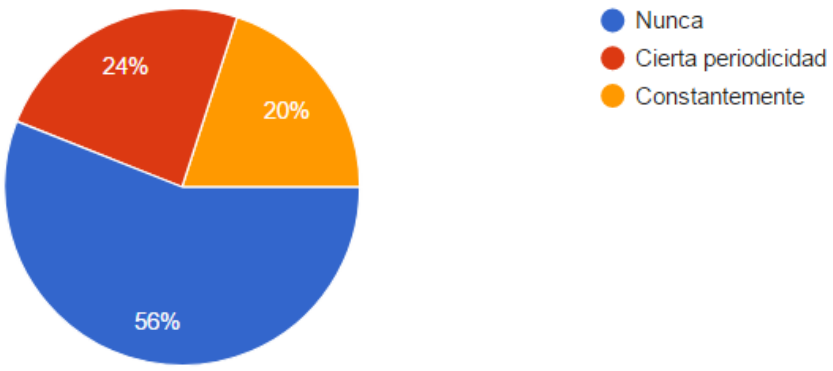
Fuente: Elaboración propia a partir del cuestionario aplicado a profesionales de seguridad informática y seguridad de la información.

La amenaza no la constituye solamente el que se utilicen dispositivos personales en el ambiente de trabajo, sino que la problemática aumenta debido a que en la actualidad según el 60% de los encuestados dentro de las instituciones no existen regulaciones asociadas con el empleo de dispositivos móviles personales en la institución, esto pone en evidencia el riesgo que existe y la necesidad de tomar acciones para atender esta situación. A su vez:

> *"A través del correo electrónico corporativo y cuentas de correo gratuitas se envía información como consecuencia de un engaño o de forma «voluntaria». Mejora con concienciación en el uso correcto del correo electrónico y si se controla la información que puede enviarse por estos medios y en qué casos debe ir cifrada."(INCIBE, 2017, p. 1)*

Respecto al uso del correo electrónico personal, un 44% admite utilizarlo para propósitos de trabajo, potenciando con esto el que incidentes por fuga de información se puedan presentar, tal y como se visualiza en el siguiente gráfico:

Figura 266. Utiliza el correo personal para propósitos laborales



Fuente: Elaboración propia a partir del cuestionario aplicado a profesionales de seguridad informática y seguridad de la información (2016).

Por otro lado, las siguientes citas ilustran situaciones riesgosas para los trabajadores y las entidades donde laboran:

"Cuando se utilizan redes inalámbricas desprotegidas, como la de los aeropuertos o los hoteles, por trabajadores de viaje sin tener en cuenta que transmiten y quién puede estar escuchando. Mejora si se conciencia a los empleados de en qué casos hacer uso de estas redes, si se controla qué información o aplicaciones se pueden usar fuera de la oficina y si se les proporciona una VPN para accesos desde el exterior.

Utilizando aplicaciones no controladas por la empresa, por ejemplo para almacenamiento en la nube (Dropbox, Google Drive, Mega) o herramientas de colaboración, mensajería instantánea o multiconferencia (Skype, Hangouts, Line, Viver,…) y otras para compartir archivos en P2P (eMule, uTorrent,…). Mejora si se establecen políticas de uso de software permitido, bloqueando su instalación o desinstalándolos.

Publicando en redes sociales información de forma inadecuada o algo que no debería publicarse, y cuando se responde a usuarios sin control. Mejora si se conciencia a los usuarios de los usos aceptables de las redes sociales, corporativas y personales, y si se centraliza en profesionales el uso de las cuentas de redes sociales corporativas.

Si resultamos infectados por malware que roba datos (troyanos, spyware, keyloggers, stealers y ransomware) nuestra información «abandonará» nuestras instalaciones o dejará de estar disponible muchas veces sin que nos demos cuenta. En este caso mejora con concienciación para evitar contagiarse y utilizando productos antimalware." (INCIBE, 2017, p. 1)

Cisco, por su parte, en su informe presentado en 2014 expone:

"Que a pesar de las políticas de seguridad, procedimientos y herramientas que se utilizan, los empleados de todo el mundo

participan en conductas de riesgo que exponen a los datos corporativos y personales."(p. 1)

Los comportamientos incluyen:

"Uso de aplicaciones no autorizadas: el 70% de los profesionales de TI cree que el uso de programas no autorizados fue responsable de hasta la mitad de los incidentes de pérdida de información en sus empresas.
Uso indebido de computadoras de la empresa: el 44% de los empleados comparte dispositivos de trabajo con otras personas sin supervisión.
Acceso no autorizado tanto físico como a través de la red: el 39% de los profesionales de TI afirmó que ha debido abordar el acceso no autorizado por parte de un empleado a zonas de la red o de las instalaciones de la empresa.
Seguridad de trabajadores remotos: el 46% de los empleados admitió haber transferido archivos entre computadoras del trabajo y personales al trabajar desde el hogar.
Uso indebido de contraseñas: el 18% de los empleados comparte contraseñas con sus colegas. El porcentaje aumenta al 25% en China, India e Italia." (CISCO, 2014, p. 1)

Es por esta razón que se considera trascendental para reducir la fuga de datos que las instituciones integren la seguridad en su cultura empresarial; además, evaluar constantemente los riesgos de cada interacción con redes, dispositivos, aplicaciones, datos y, por supuesto, otros usuarios.

Según el Instituto Nacional de Ciberseguridad (INCIBE, 2016) las causas de la fuga de datos se clasifican de la siguiente forma:

“Aquellas que pertenecen al ámbito organizativo y aquellas que hacen referencia al ámbito técnico. Para INCIBE, la mayoría de las causas, tanto organizativas o técnicas, generalmente, implican la ausencia de algún tipo de medida de seguridad, procedimiento, herramienta, etc. Esta ausencia de medidas supone la falta de control sobre la información y esta falta de control aumenta de forma significativa la probabilidad de que se produzca un incidente de fuga de informació.”. (p. 7)

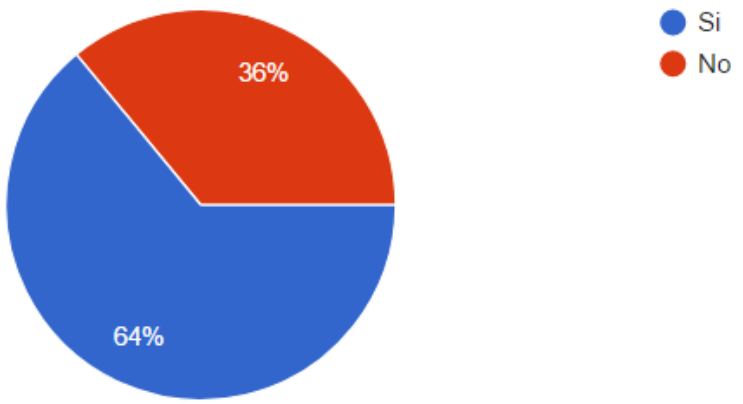
Causas organizativas:

- **Falta de una clasificación:** esta clasificación se puede realizar con base en su nivel de confidencialidad, en función de diversos parámetros: el valor que tiene para la organización, el impacto que puede generar su filtración, su nivel de sensibilidad o si se trata de información personal o no. Si se desconoce el valor de la información que trata la entidad, no será posible diseñar y seleccionar las medidas de protección adecuadas. Por otro lado, el ámbito de difusión permite establecer el perímetro dentro del cual podrá ser difundida la información y junto con el nivel de confidencialidad, hará posible determinar quién debe conocer la información y qué tipo de acciones puede realizar sobre esta. Esto se conoce como principio del mínimo conocimiento.
- **Los errores o la falta de conocimiento y formación**: para esto es necesario utilizar de forma responsable los recursos que la organización pone a su disposición (los servicios en la nube, los dispositivos móviles, el correo electrónico, la navegación web, etc.) Por otro lado, debe disponer de ciertos conocimientos y formación sobre su actividad diaria y en materia de ciberseguridad, siendo responsabilidad de la entidad proporcionar la formación necesaria de manera que el empleado pueda desempeñar su función de forma segura.

- **Ausencia de procedimientos y el establecimiento de pautas y obligaciones para los trabajadores en el ámbito de ciberseguridad:** El establecimiento de políticas que indiquen al usuario claramente cuáles son los límites dentro de los cuales deberán desempeñar su actividad y, por otro lado, los procedimientos para aquellas actividades de especial importancia o riesgo, disminuirán el riesgo para que se produzca una fuga de información.

De la mano con la existencia de políticas y lineamentos dentro de las instituciones, existe un aspecto de principal trascendencia que debe considerarse y se basa en el hecho de que es igual de importante que se desarrolle una política o directriz y que la conozca todo el personal.

Figura 277. Existencia de políticas de seguridad o lineamientos



Fuente: Elaboración propia a partir del cuestionario aplicado a profesionales de seguridad informática y seguridad de la información (2016).

Como se aprecia en el anterior gráfico, existe un 36% que afirma que los documentos que se desarrollan y en los cuales se invierte muchos esfuerzos y recursos (humanos, financieros, entre otros) no son de conocimiento de toda la institución, lo cual deja en evidencia problemas de comunicación que existen dentro de las instituciones.

Adicionalmente, se puede afirmar que los esfuerzos para divulgar son diversos y no responden a un objetivo coordinado, por lo cual este también es un tema que debe contemplarse y atenderse.

Es importante recalcar que es tan importante el desarrollo de lineamientos y políticas que se deben seguir dentro de las instituciones, así como que se comuniquen asertivamente, pues de no ser así no se tendría un beneficio total de lo que se quiere y por lo que se han dedicado tantos esfuerzos y recursos en su desarrollo, además de que evidenciaría un sector de la institución que es víctima potencial y vulnerable por su desconocimiento del tema.

- **No contar con acuerdos de confidencialidad de la información con los empleados:** es importante solicitar por escrito la conformidad con diversas normas internas, como la política de confidencialidad o de seguridad, entre otras, de manera que el futuro empleado deje por escrito la aceptación de las condiciones correspondientes. Además, se cuenta con legislación que permite establecer límites legales a las actividades de sus trabajadores y que pueden ser utilizadas como mecanismos de disuasión para evitar un uso malintencionado de la información.

Causas técnicas:

- **El código malicioso o malware: d**iseñado para mantener oculto su código en un sistema, mientras recoge y envía información.
- **El acceso no autorizado a sistemas e infraestructuras: y**a sea como parte de una campaña de desprestigio, con el acceso no autorizado a una página web de una organización, o con motivo de sustraer información sobre secretos industriales, gran parte de estos accesos no autorizados se podrían evitar si los sistemas y aplicaciones estuvieran convenientemente actualizados. La actualización se considera parte fundamental de una buena aplicación, puesto que aporta mayor

seguridad y denota un trabajo de mejora continua que redunda en beneficio de la aplicación y, por ende, del usuario.

- **El uso de servicios en la nube para el almacenamiento:** el nivel de seguridad que tiene es el del eslabón más débil (muy a menudo son los propios usuarios y sus contraseñas).
- **El uso de las tecnologías móviles para el trabajo diario:** aunque se utilicen medidas como el cifrado de los dispositivos o el uso de VPN (redes privadas virtuales) en las comunicaciones, ninguna medida puede llegar a ser suficiente para asegurar entornos que almacenen información muy crítica. Un dispositivo sustraído, en las manos equivocadas podría ocasionar un impacto muy grande a la institución.

Los resultados anteriores dejan en evidencia situaciones como:

- Falta de capacitación y concientización del personal encargado de atender el tema de seguridad informática y seguridad de la información en algunas áreas.
- Las instituciones están completamente expuestas a que se produzca una fuga de datos a través de metadatos contenidos en documentos de acceso público.
- Las fugas de datos a nivel general por aspectos no asociados a metadatos aún no se atienden adecuadamente, posiblemente porque se carece de los recursos (personales, económicos y equipos) destinados para este fin.
- Al no atenderse el tema de fuga de datos que pueda producirse a través de metadatos, están evidenciando falencias que pueden generar consecuencias (reputacionales, legales, económicas) a nivel institucional.

4.3.5 Estrategia 5:

Modelo para la prevención de la fuga de datos que se produce a través de metadatos, basado en buenas prácticas de seguridad de la información.

Referente a la estrategia 5, se utiliza como instrumentos las entrevistas y el cuestionario, ambos dirigidos a los profesionales de seguridad informática y personal de TI; el análisis bibliográfico; el juicio de profesionales expertos en seguridad de la información; así como la utilización de aplicaciones de software utilizadas para detectar la existencia de metadatos.

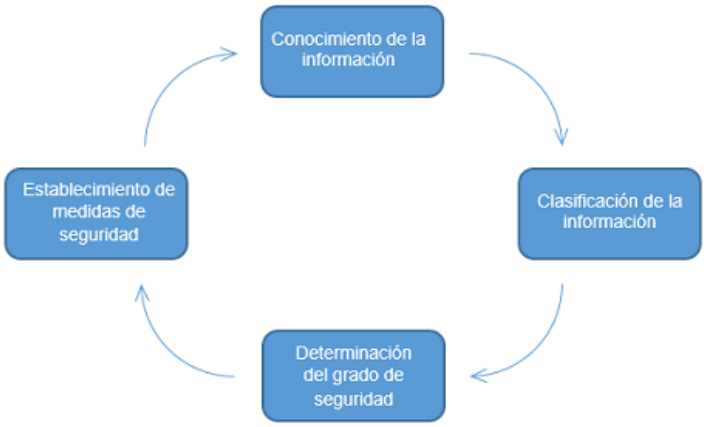
Objetivo: Propuesta de modelo para la prevención de la fuga de datos que se produce a través de metadatos, basado en buenas prácticas de seguridad de la información.

El Instituto Nacional de Ciberseguridad (INCIBE, 2016) propone la siguiente alternativa para prevenir una fuga de información dentro de la empresa.

> *"Para prevenir con garantía este tipo de incidentes, debemos tener en cuenta el tipo y el valor de la información a proteger, teniendo en cuenta el posible impacto que pueda causar en nuestro negocio su robo o pérdida, ya que puede tener distintas consecuencias en función del tipo de información y del tipo de organización. Por lo tanto, siempre debemos:*
>
> - *Conocer la información que gestiona la organización. Esto debe hacerse a través de entrevistas y reuniones con el personal de la organización.*
> - *Clasificarla según su criticidad, según un criterio razonable y unificado.*
> - *Determinar su grado de seguridad: ¿es alto el riesgo de pérdida de información?, ¿y el de fuga o robo de información?, ¿puede ser alterada sin autorización?*

- *Establecer las medidas necesarias para mejorar su seguridad." (p. 1)*

Figura 288. Alternativa para prevenir una fuga de información



Fuente: INCIBE, 2016.

Además, indica que para reducir la probabilidad de que este tipo de incidentes ocurran, podemos establecer diferentes tipos de medidas entre las que se destacan:

- **Técnicas:** medidas básicas que podemos aplicar, independientemente del tamaño de la empresa, como por ejemplo:
  - Cifrado de la información confidencial corporativa.
  - Instalación, configuración y actualización de cortafuegos.
  - Mantener actualizadas todas las aplicaciones de nuestros sistemas, entre otros.

Para empresas con mayores recursos económicos o que necesitan un nivel mayor de exigencia se pueden aplicar otras medidas más avanzadas, como por ejemplo:

  - Soluciones de prevención de pérdida de datos o DLP (del inglés Data Loss Prevention) que suelen estar orientadas a la monitorización y control.

  - Las destinadas a la gestión del ciclo de vida de la información o ILM (del inglés Information Lifecycle Management) desde que esta es generada o elaborada hasta su archivado o destrucción final.

  - Las herramientas de control de dispositivos externos de almacenamiento, que están destinadas a controlar el acceso físico a puertos y dispositivos extraíbles como USB para evitar fugas de información.

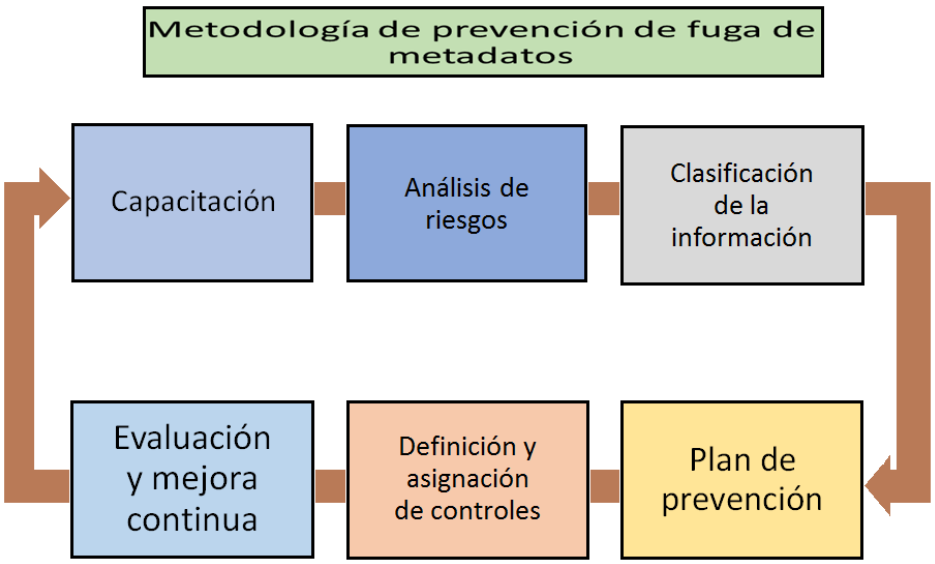
- **Organizativas:** este tipo de medidas están estrechamente relacionadas con «la forma» en que se maneja o se trata la información, situaciones que suelen darse por falta de conocimiento del usuario. Por este motivo, es importante fijar políticas de seguridad, junto con acciones de concienciación a todos los empleados.

- **Jurídicas:** es importante que los empleados o proveedores que gestionan la información corporativa cumplan las políticas de seguridad; para ello, podemos firmar acuerdos de nivel de servicio (SLA) con los proveedores y hacer que los usuarios firmen unos acuerdos de confidencialidad, en los que los que regularemos los aspectos relativos a la seguridad y la confidencialidad de la información en la prestación de un servicio, incluyendo las sanciones en caso de incumplimiento. Un punto importante, y de obligado

cumplimiento, es el relacionado con el tratamiento de ficheros que contienen datos de carácter personal.(INCIBE, 2016).

Considera también que estos incidentes en su mayoría generan un impacto reputacional. Lo anterior, sin duda, puede contribuir en la prevención de la fuga de datos, pero desde una perspectiva general. En todo caso, no atiende la fuga que se produce por metadatos contenidos en documentos de acceso público. Para atender este escenario se propone utilizar el siguiente modelo:

Figura 299. Metodología de prevención de fuga de datos causada por metadatos



Fuente: Elaboración propia, 2017.

Prevención de la fuga de datos

1. **Capacitación al personal**

   Deben existir procesos de concientización y capacitación que incluyan a todos los niveles de la entidad, con la finalidad de que se atienda en todo momento (incluso desde el diseño) aspectos asociados a la seguridad, que permitan atender la existencia o eliminación de metadatos en los documentos.

2. **Análisis de riesgos:**
    - Se deben identificar los activos críticos de información y sus riesgos asociados.
    - Antes de elegir qué va a proteger y cómo lo va a hacer, es importante realizar un análisis objetivo de los riesgos que enfrenta su información (los metadatos).
    - Es importante lograr un consenso a nivel institucional relacionado a los riesgos que se deberán atender en el corto, mediano y largo plazo.
3. **Clasificación de la información:**
    - Determinar el nivel de protección necesario para los activos de información.
    - Establecer criterios de clasificación objetivos y claros, acordados con los dueños (responsables) de la información.
    - Crear esquemas o estándares en cuanto a la descripción de los metadatos cuando se están creando los documentos y, aunque no necesariamente sea la mejor práctica, deberían ser eliminarlos.
    - Acordar los requerimientos mínimos para el tratamiento durante todo el ciclo de vida de la información:
        a. Obtención.
        b. Uso.
        c. Divulgación.
        d. Almacenamiento.
4. **Elaborar plan de prevención:**

    Este plan de prevención debe identificar y documentar cada una de alternativas, así como sus estrategias para administrar (aceptar[6], reducir, mitigar o transferir) los riesgos principales, de acuerdo con lo establecido en los pasos previos.

[6]Es importante realizar una definición formal de aquellos riesgos que se aceptarán por los dueños o responsables de la información

5. **Definición y asignación de controles:**
    - Se deben establecer los controles necesarios según capacidades institucionales. Por ejemplo, podría utilizarse un análisis (costo/beneficio).
    - Se debe valorar por las instituciones la aplicación de mecanismos (herramientas) que permitan retirar de los documentos los metadatos, con excepción de que dicha información sea necesario mantenerla o comunicarla.
6. **Evaluación y mejora continua:**
    - Se deben probar los controles implementados.
    - Identificar las fallas existentes en el diseño y operación, así como realizar los ajustes correspondientes a fin de que los controles funcionen adecuadamente y con esto se logre la eliminación total de los metadatos contenidos de documentos de acceso público.

CAPÍTULO V

PROPUESTA DE SOLUCIÓN

Se recrea un escenario, con el fin de evidenciar la situación o problemática que se evidencia y posteriormente se muestran alternativas que puedan atender la ocurrencia de fugas de datos que se producen a través de metadatos contenidos en documentos de acceso público.

Paso 1: Obtener la información

Descripción:

Para la obtención de la muestra, se realizarán procedimientos simples que pudiesen realizar o recrear usuarios sin mayor especialización, pero que le permitan obtener información relevante.

Escenario

Se atenderán dos escenarios principalmente.

1. Se accederá a sitios web de instituciones públicas y de ahí se descargarán 10 documentos cualesquiera que estén al alcance (disponibles) de cualquier usuario.

2. Se utilizará una técnica informática que consiste en filtrar información en un buscador (Google, Bing). Esto permite obtener de una forma más rápida los resultados que se tuvieron en el punto 1.

Por ejemplo: para buscar en Google tipos de archivo de documentos de texto (.doc, docx,), de hojas de cálculo (.xls, .xlsx) o formato de documento portable (.pdf) que se encuentran en el sitio web de alguna institución pública de Costa Rica, solo tendríamos que utilizar lo siguiente:

- Ingresar al buscador www.google.com
- Definir el tipo de Archivo a buscar – “Filetype:doc”
- Definir el sitio web– “Site: ejemplo.com”

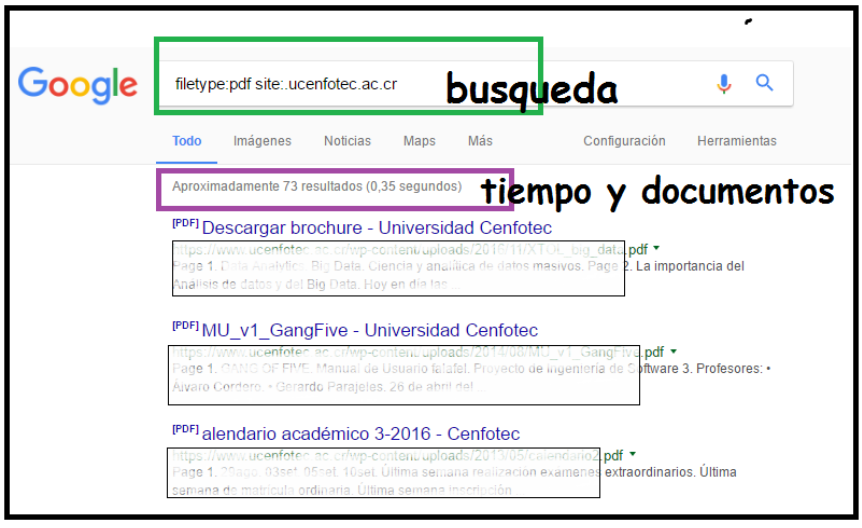
Posterior a esto, aparecerán los resultados y, de esta forma, descargaría(guardaría) los que se considere pertinente.

Ejercicio:

Para buscar los documentos en formato portable que se encuentran en el sitio web de la Universidad CENFOTEC, se aplica en el buscador de Google lo siguiente:

“filetype:pdfsite:.ucenfotec.ac.cr”

Figura 300. Escenario de ejemplo de búsqueda de metadatos



Fuente: Elaboración propia, 2017.

Similar a los dos escenarios anteriormente descritos, este procedimiento se aplicó para obtener los metadatos contenidos en documentos de acceso público que están disponibles en sitios web de Instituciones Públicas en Costa Rica.

Paso 2: Alternativas de solución para limpieza de documentos

El proceso de limpieza de documentos:

"Consiste en retirar de estos toda la información adicional contenida en campos ocultos, metadatos, comentarios o revisiones anteriores, salvo cuando dicha información sea pertinente para el receptor del documento" (García, Blázquez y Chema Alonso, 2011, p. 218)

Además, los autores indican lo siguiente:

"Esta medida es especialmente relevante cuando el documento se difunde ampliamente, como ocurre si se ofrece al público en un servidor web u otro tipo de repositorio de información.

Y se tiene que tener presente que el incumplimiento de esa medida puede perjudicar:

- *Al mantenimiento de la confidencialidad de información que no debería haberse revelado al receptor del documento.*
- *Al mantenimiento de la confidencialidad de las fuentes u orígenes de la información que o debe conocer el receptor del documento.*
- *A la buena imagen de la organización que difunde el documento por cuanto demuestra un descuido en su buen hacer."(García, Blázquez y Chema Alonso, 2011, p. 219)*

La opción de automatización resulta muy interesante puesto que independiza la seguridad del buen hacer del usuario. Aunque los usuarios sean conscientes de la necesidad, desafortunadamente se enfrentan a que, en el trabajo diario, esta limpieza no siempre se realiza, o bien no se hace correctamente.

Eliminación de metadatos en documentos

Para comenzar con el proceso de eliminación de metadatos, se debe conocer qué son éstos y cuál es la importancia de proceder a suprimirlos.

¿Qué es un metadato?

En general, se desconoce que aparte de la información “visible” de las fotos y documentos, existen otros datos que están incluidos y que pueden ser fácilmente visibles por cualquier persona que tenga acceso a ellos.

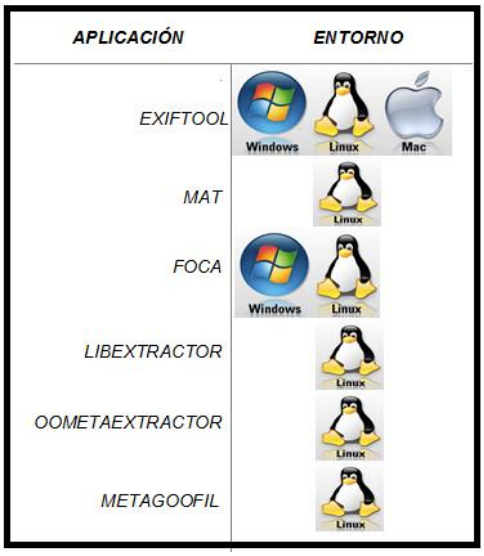
Los metadatos constituyen la información que es incluida dentro de los archivos digitales por el software de edición o creación de estos. Contienen información diversa: fecha de creación del archivo, nombre de autor, autores anteriores, nombre de la compañía, fecha de última modificación, las coordenadas de la ubicación en que se encontraba cuando por ejemplo se tomó alguna foto, entre otros.

¿Por qué es necesario eliminar estos metadatos?

Así como algunos de los metadatos obtenidos pueden ser intrascendentes, otros pueden servir como base para realizar procesos de ingeniería social, ataques de fuerza bruta, por mencionar algunos; quien tenga acceso a estos metadatos podría obtener los nombres de posibles usuarios, sistema operativo, nombres de red, entre otros. De ahí que deba considerarse por cada institución si es necesario almacenarlos cuando se están creando los documentos, o si por el contrario la institución deberá tener procedimientos desarrollados para su eliminación.

Existen diferentes herramientas que permiten realizar el borrado de metadatos y a continuación se describen en la siguiente figura.

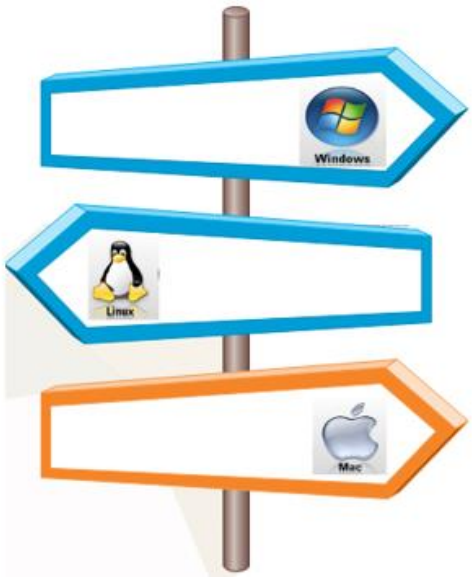
Figura 311. Herramientas para el borrado (eliminación) de metadatos



Fuente: Elaboración propia, 2017.

Cada aplicación que se describe a continuación se puede utilizar en uno o varios sistemas operativos o plataformas.

Figura 322. Sistemas operativos donde se utilizan las herramientas de borrado de metadatos



Fuente: Elaboración propia, 2017.

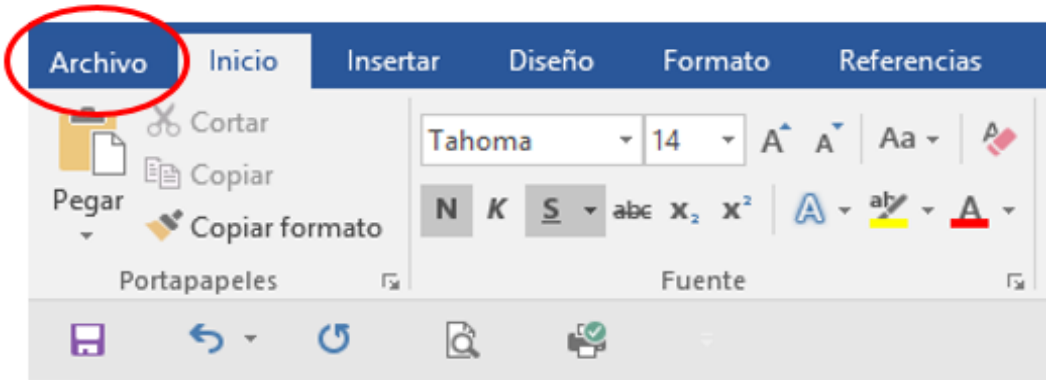
A continuación, se describen los pasos a seguir en el proceso de eliminación de metadatos según la plataforma en que se esté trabajando.

I. Herramienta para la eliminación de metadatos contenida en las aplicaciones de la suite de Microsoft Office

Para realizar el borrado de los metadatos contenidos en los documentos creados con las aplicaciones propietarias de Microsoft (Power Point, Word, Excel), se procederá de la siguiente manera:

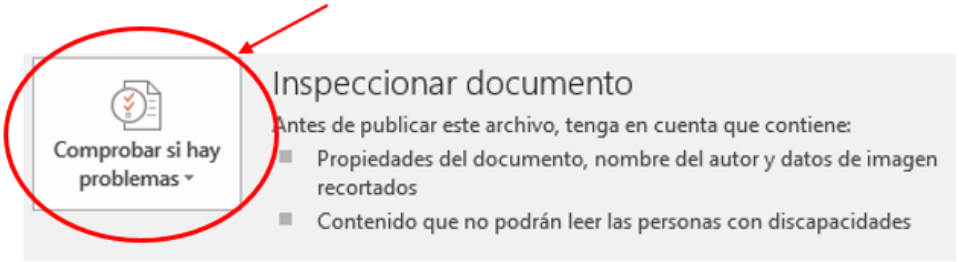
1. Se ingresa al programa con el cual se creó el documento al cual se desea eliminarle los datos, ya sea Word, Excel o Power Point, y se abre dicho documento.

2. Estando dentro del documento, se procede a hacer clic en el menú “Archivo”, situado en la esquina superior izquierda de la cinta de opciones.

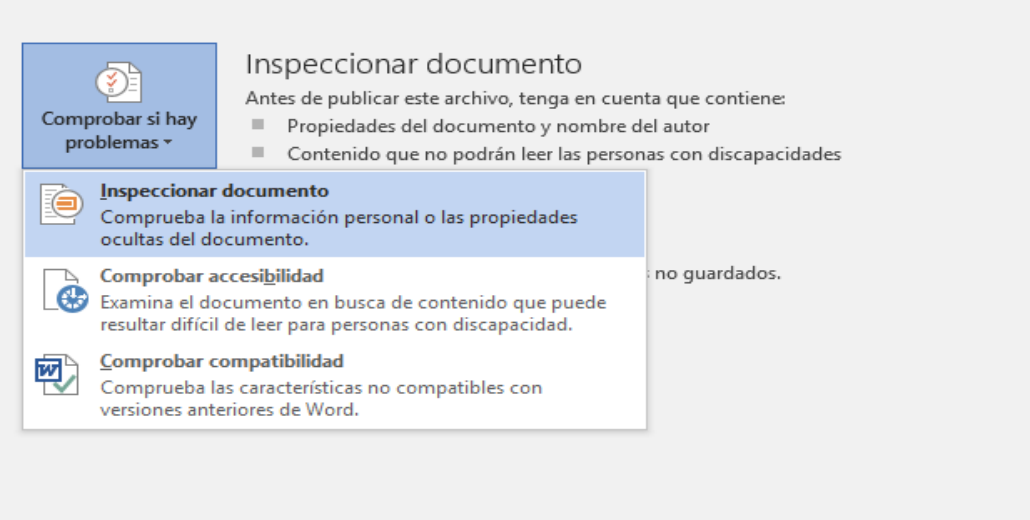


3. Habiendo hecho esto se desplegará la siguiente pantalla**:**

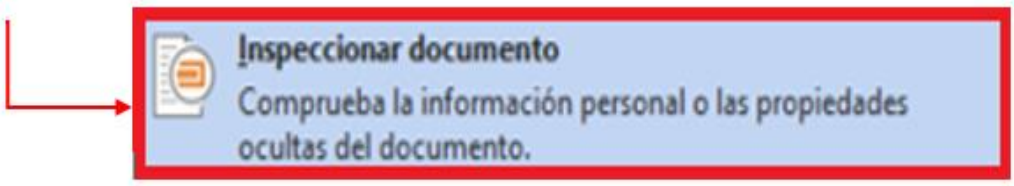
4. En esta pantalla se hace clic en el botón intermedio que dice “Comprobar si hay problemas”



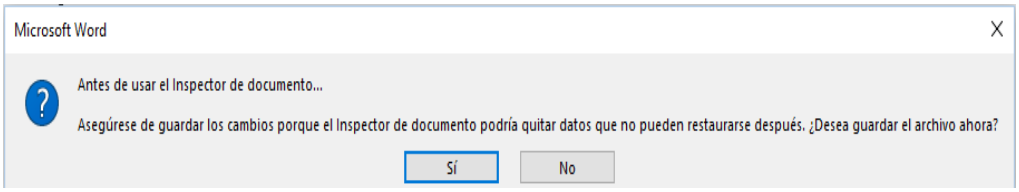
5. Al presionar dicho botón, en la parte inferior de éste se desplegarán las siguientes opciones:



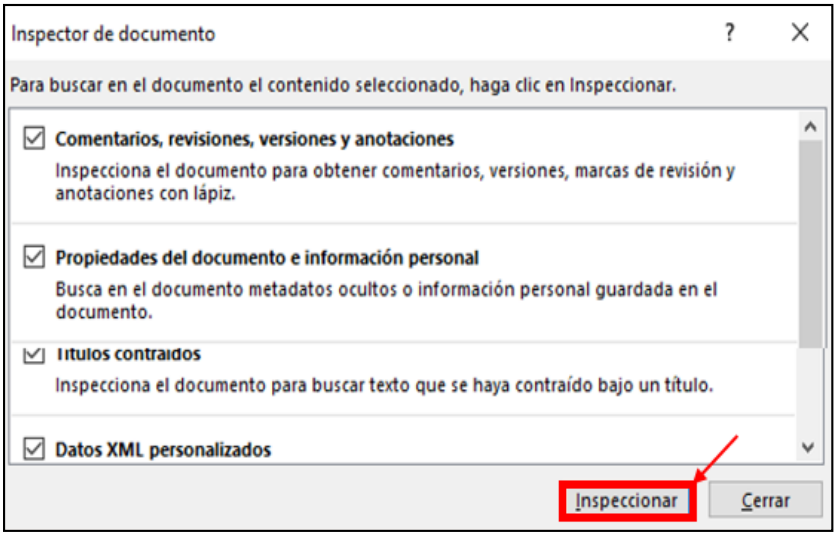
Se seleccionará entonces la primera opción, denominada **"Inspeccionar documento"**



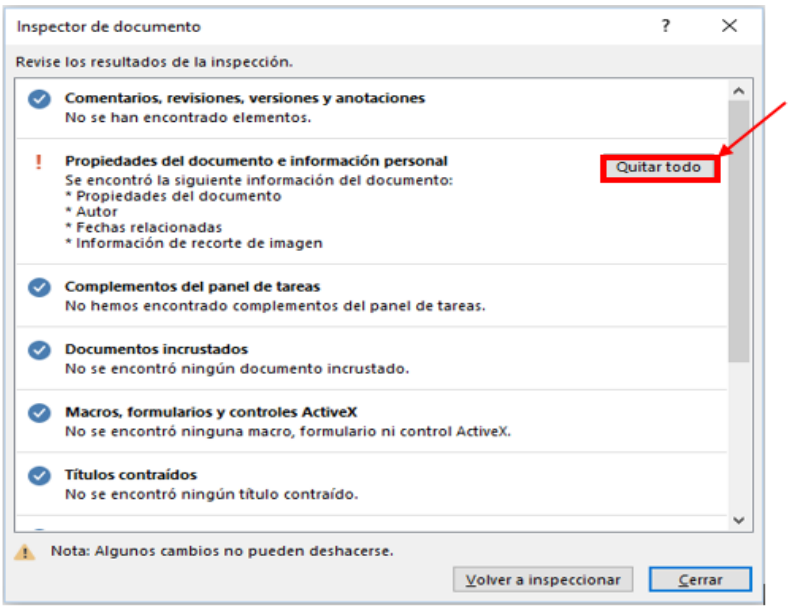
6. Si no ha salvado el archivo, aparecerá una ventana de confirmación solicitando si desea salvar el archivo, al responder que **SÍ**, se guarda el archivo y se prosigue mostrando la ventana denominada **"Inspector de documento".**



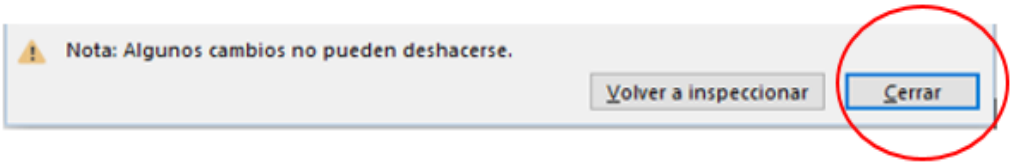
7. En esta ventana aparecerá una lista de las diferentes características que el programa inspeccionará, así que se hace clic en el botón **"Inspeccionar"** que se encuentra al final de esta ventana**.**



8. Posterior a esto aparecerá una ventana con los resultados de la inspección; así que a cada lado de los aspectos analizados y que contienen metadatos aparecerá un botón que tiene por título **"Quitar todo",** se hace clic sobre este botón en todos los ítems donde aparezca.



9. Para cerrar esta ventana se hace clic en el botón **"Cerrar"** ubicado en la esquina inferior derecha de esta ventana.



10. Completados estos pasos ya se habrán eliminado los metadatos del documento, pero es necesario que se **GUARDE EL DOCUMENTO** para asegurar la eliminación (remoción) de los metadatos.

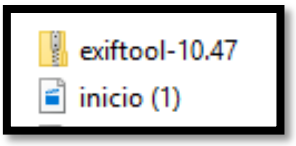
II. Herramienta para la eliminación de metadatos ExifTool

Exiftool es un programa con el cual se puede leer, escribir o borrar los metadatos de los archivos con diferentes formatos (JPEG, PNG, MP3, PDF, WEBM, RAR, RTF, SWF, RAW, PSD o PSP) incluyendo archivos de video,

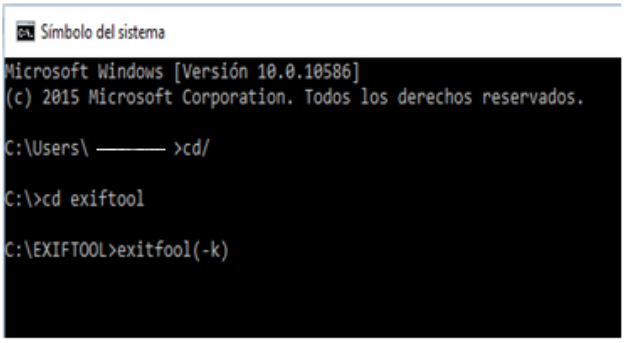
sonido, imágenes o texto. Existen versiones para Sistemas operativos Microsoft Windows, Linux y Macintosh descargables de forma gratuita desde la página principal del autor.

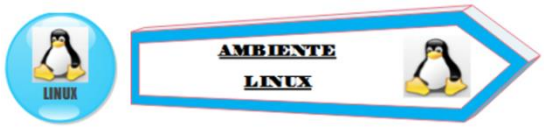
Descargar la herramienta gratuita directamente de la página del autor (Windows Executable: exiftool-10.47.zip 5.8MB). **DESCARGA A TRAVÉS DE: http://www.sno.phy.queensu.ca/~phil/exiftool/**

1. El archivo tiene una extensión ".zip" que contiene la versión más actualizada de la aplicación, que en este caso es la 10.47, la cual se puede descomprimir en cualquier directorio deseado.



2. El archivo descomprimido será **exiftool(-k).exe** que se usará través de la ventana de comandos.
3. Para acceder y abrir la consola (terminal) lo más cómodo es pulsar la combinación de teclas `Tecla Windows + R` , o el símbolo de Windows  , se escribe `cmd` y se preciona Enter.
4. Es necesario ubicarse en el directorio donde se copia el **archivo.exe** y se escribe en la línea de comandos el nombre del ejecutable.





1. Los usuarios de Linux deben tener instalado Perl 5.004 o superior.
2. En Linux se puede utilizar esta herramienta; por ejemplo, en Ubuntu se realiza la instalación con el siguiente comando:

   # apt-get install libimage-exiftool-perl

1. Descargar la herramienta gratuita directamente de la página del autor (Mac OS X Packege: ExifTool-1047.dmg 2.6MB).
2. **Se instala como un programa normal** (abrir el archivo del disco, presionar doble clic en el paquete de instalación y seguir las instrucciones).
3. Puede ejecutar exiftool al digitar "**exiftool**" en un terminal.

En resumen, en cualquiera de las plataformas anteriormente descritas (Linux, Microsoft Windows y Masintoch), la sintaxis utilizada para el borrado de metadatos sería la siguiente:

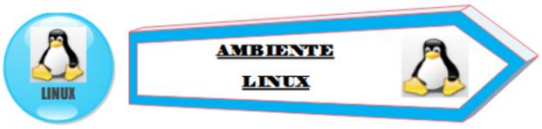
"**ExifTool –all**= ***ruta/nombre del archivo (con extensión)"***

¿Y SI SE NECESITA EL DOCUMENTO ORIGINAL?

Al realizar el borrado de los metadatos se crea un archivo con el nombre original pero terminado en "._original", que es una copia de seguridad del archivo original incluyendo sus metadatos para situaciones en la que resulte necesario utilizarlo.

III. Herramienta para la eliminación de metadatos MAT

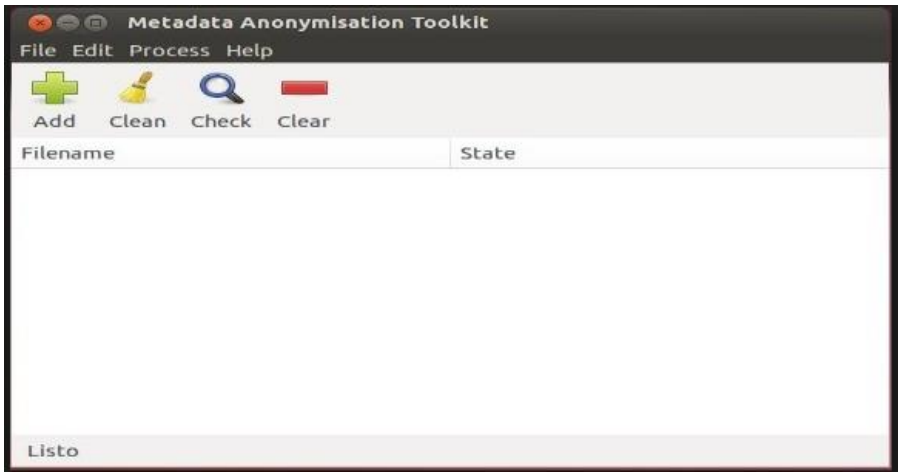
MAT (Metadata Anonymisation Toolkit) es una herramienta desarrollada en el lenguaje de programación Python, se utiliza para limpieza de metadatos, esta aplicación de incluye por defecto en sistemas operativos como “TAILS” y en los repositorios del sistema operativo Debian. **DESCARGA A TRAVÉS DE:** **https://mat.boumorg/**



1. Se puede descargar del link indicado anteriormente, pero normalmente se encuentra en sistemas operativos Linux como: Debian y Ubuntu, por lo cual se puede instalar sin complicaciones.
2. Para instalar el paquete se escribe el comando:

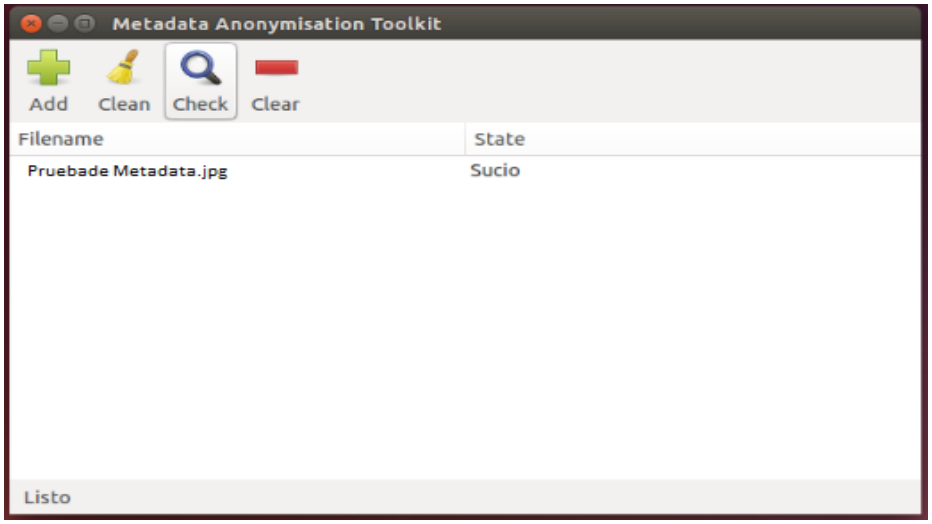
   “sudo aptitude install mat”

3. Una vez instalado, se abre y muestra una interfaz muy sencilla e intuitiva:

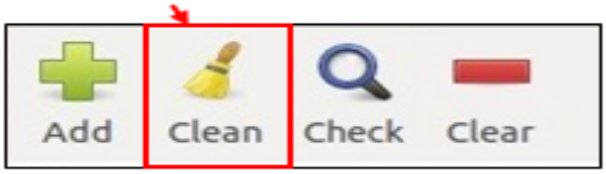


4. El archivo al que se desee eliminarle los metadatos tiene que ser elegido oprimiendo primero el botón **Add** y posteriormente seleccionando el archivo deseado.

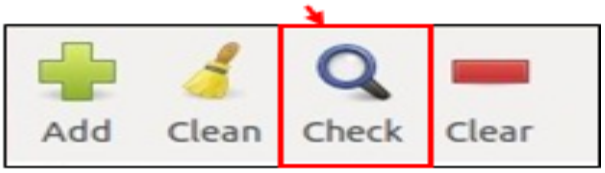
5. En la columna de **State** aparecerá la palabra "**Clean**" o "**Limpio**" si el archivo no contiene metadatos; y por el contrario aparecerá la palabra "**Dirty**" o "**Sucio**" si el archivo contiene metadatos.



6. **Clean** sirve para limpiar los metadatos del archivo que se desea borrar.



7. La opción **Check** permitirá saber si el archivo está limpio o sucio.



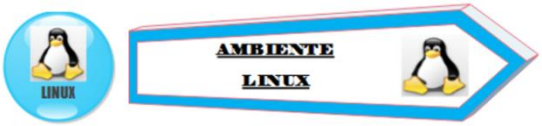
8. Y la opción **Clear** es para quitar el archivo del programa MAT una vez que se ha limpiado.

IV. Herramienta para la eliminación de metadatos FOCA

FOCA (Fingerprinting Organizations with Collected Archives) es una herramienta que fue desarrollada inicialmente por Informática64, con el propósito de realizar análisis de auditorías y análisis de pruebas de penetración.

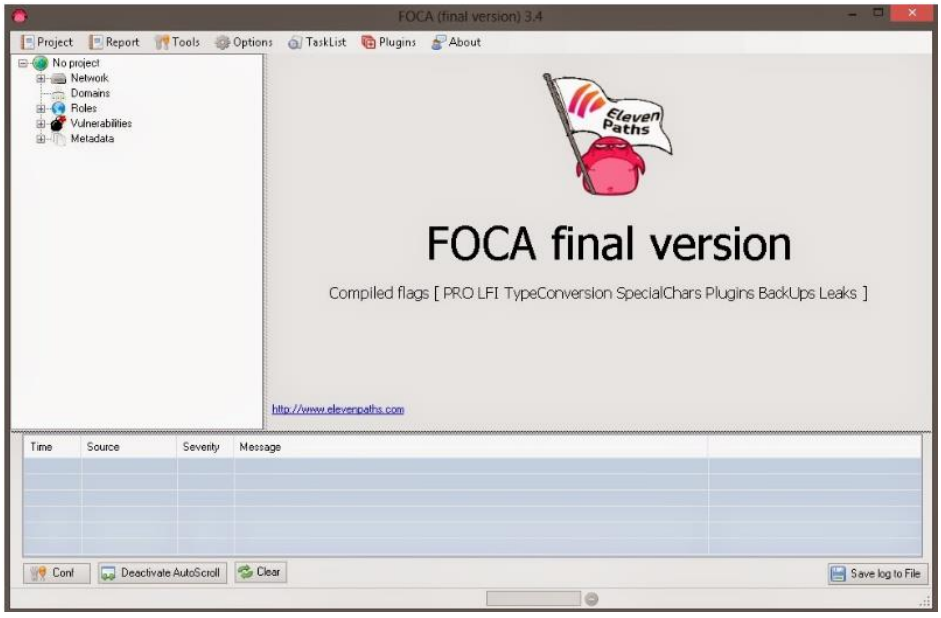
FOCA empezó a ser conocida por la posibilidad que tiene de extraer metadatos de documentos; pero, esta herramienta no solo realiza esta función, además, puede utilizarse entre otras cosas para búsquedas de servidores, dominios, URLs y documentos publicados, así como el descubrimiento de versiones de software en servidores y estaciones de trabajo (clientes).

DESCARGA A TRAVÉS DE: https://www.elevenpaths.com/es/labstools/foca-2/index.html#



Como lo describe su autor en su página web FOCA (Fingerprinting Organizations with Collected Archives), es una herramienta utilizada principalmente para encontrar metadatos e información oculta en los documentos que examina.

Los documentos que es capaz de analizar son muy variados, siendo los más comunes los archivos de Microsoft Office, Open Office, o ficheros PDF, aunque también analiza ficheros de Adobe InDesign o svg, por ejemplo.

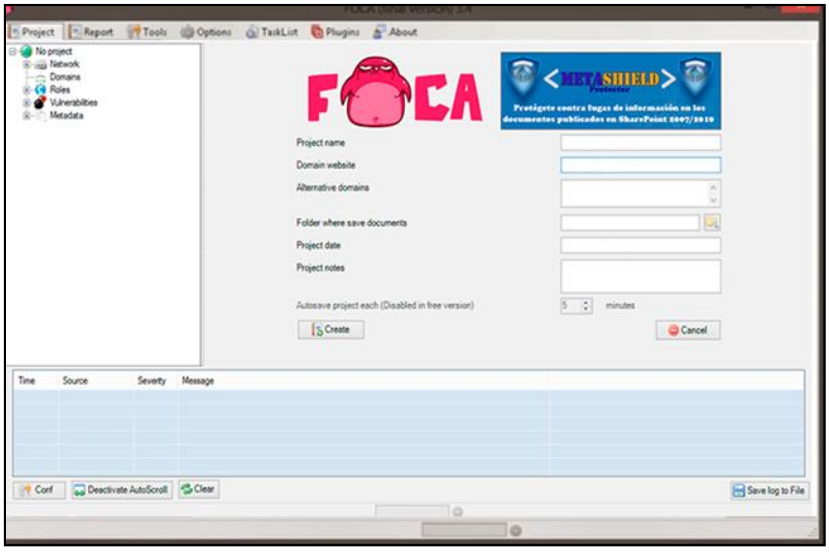


La función principal y más conocida de FOCA es la extracción de metadatos. Para extraer los metadatos de los archivos hay dos opciones para incluirlos en el análisis, dependiendo de si están guardados en nuestro computador o si están alojados en una página web externa.

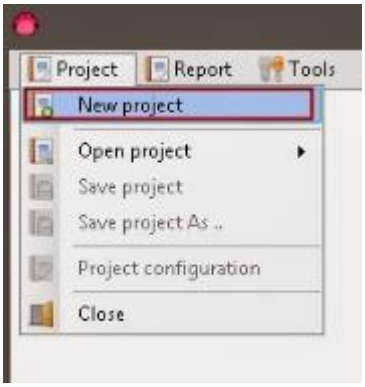
Si los archivos por analizar están en la computadora, simplemente se arrastran a la ventana de FOCA para revisarlos directamente.

A continuación se presenta el proceso de la exploración si los archivos están en un sitio web, FOCA ofrece la posibilidad de descargarlos todos juntos.

Esta será la interfaz básica en todas las versiones.



En el menú Project se selecciona la pestaña ***New Project***.

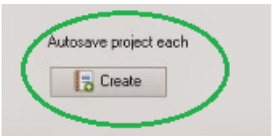


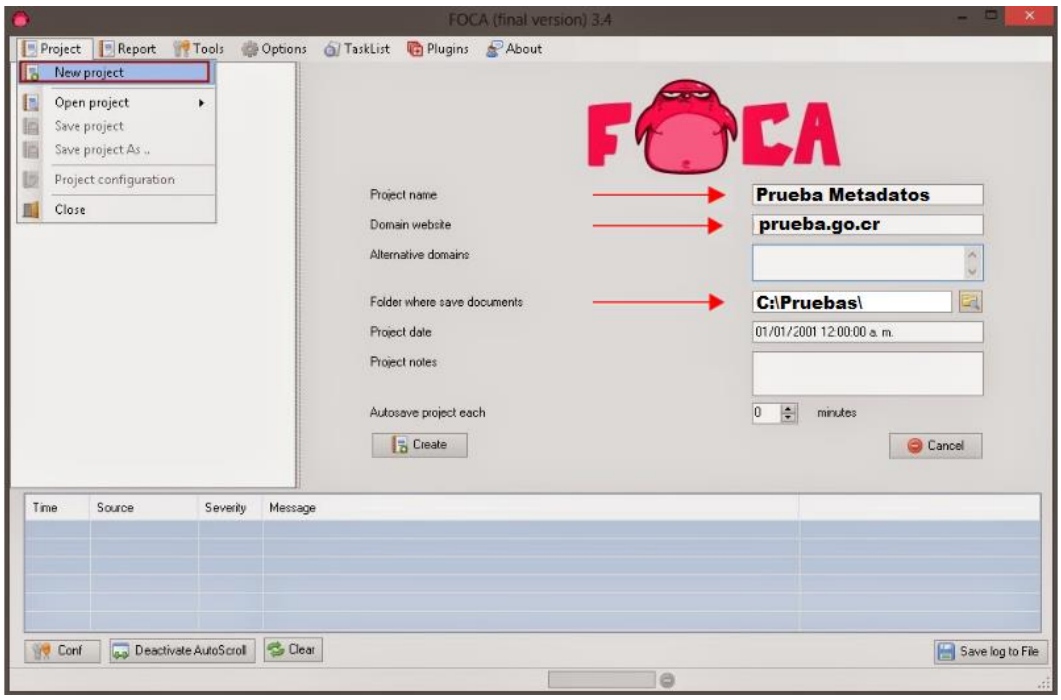
1. En el panel de la derecha, en el espacio para **Project Name** se coloca un nombre al proyecto.

2. Se anota en el espacio **Domain website** la **url** a evaluar (por ejemplo: mipagina.com)

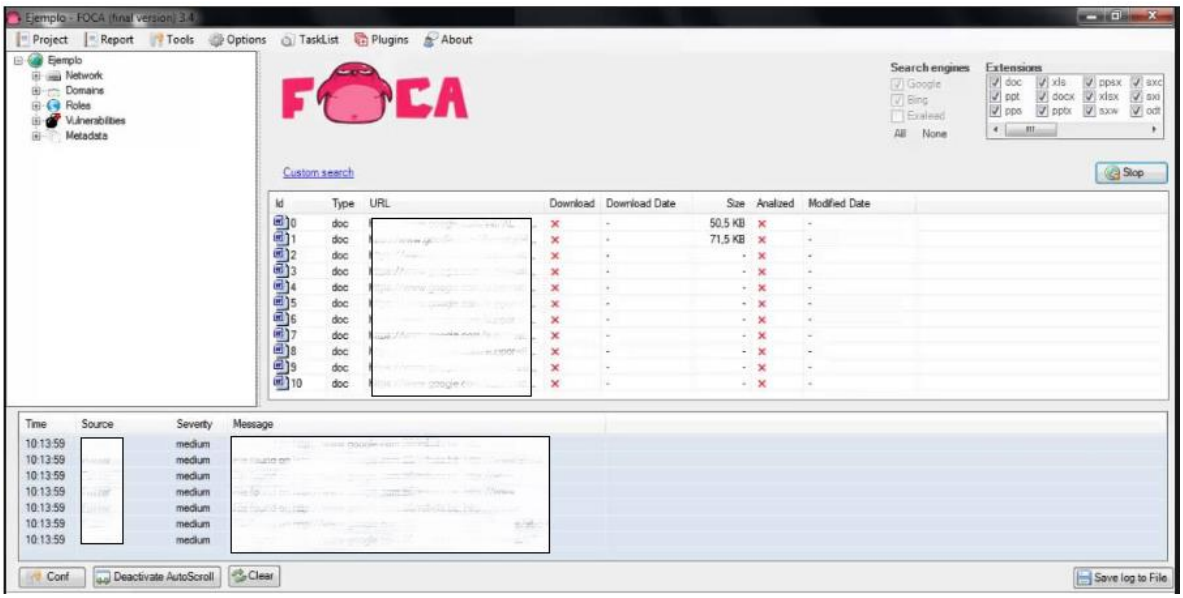
3. En el espacio denominado "**Folder where save documents**" se selecciona haciendo clic en el botón de la derecha el directorio donde se salvarán los documentos.

4. Se hace clic en el botón **Create** (Crear).

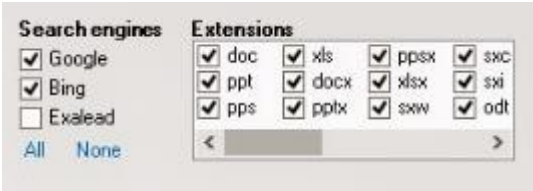




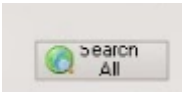
Incluso, se pueden explorar los documentos por tipo incluidos en una **url** específica usando la expresión: **“filetype: .pdf site: .prueba.go.cr”**



5. Una vez creado el proyecto se podrán seleccionar las opciones "**Searchengines**" y "**Extensions**", ahí es donde se deberán seleccionar los **buscadores** y las **extensiones** de los archivos que se buscarán.

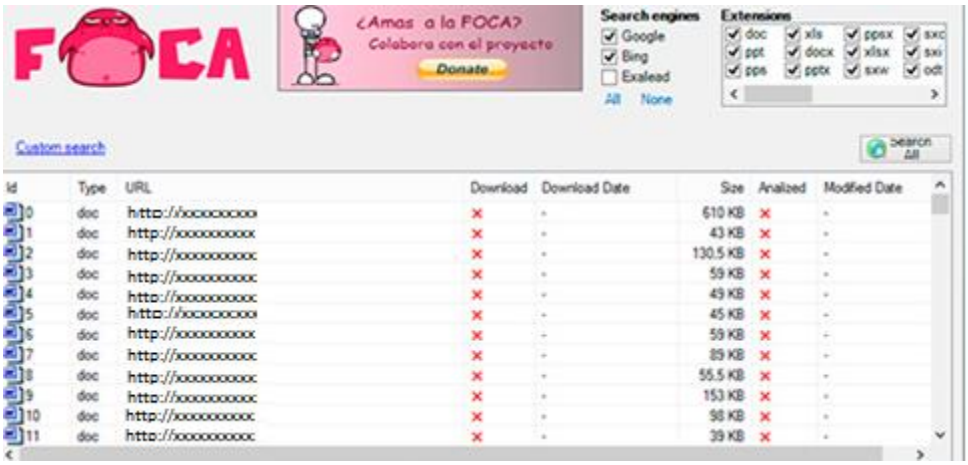


6. Se hace clic al botón **SearchAll** y comenzará la búsqueda.

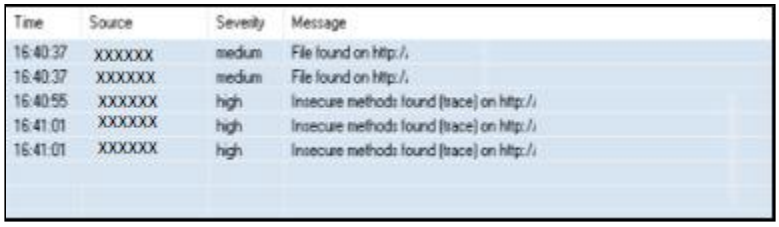


Para descargar todos los archivos, se hace clic con el botón secundario del mouse y se selecciona la opción **DownloadAll.**

7. Una vez descargados los archivos se hace clic derecho en cualquiera de ellos y se selecciona **ExtractAllMetadata** para comenzar **el análisis**. En la ventana superior aparece el identificador.

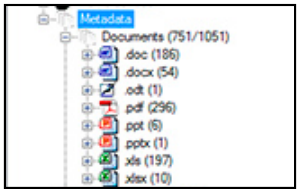


8. En la ventana inferior de la aplicación aparecerán los documentos escaneados, señalando la seriedad o gravedad del riesgo encontrado.

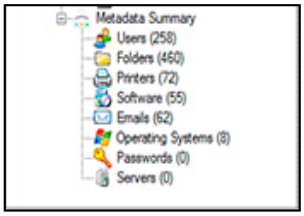


9. En la parte de la izquierda del programa existe un menú que incluye entre otras opciones **Metadata**

10. Si se da click en la opción **Metadata,** se desplegarán dos opciones: **Documents y MetadataSummary,** es en ambas opciones donde se van clasificando los archivos que están siendo descargados por la herramienta.
11. Mientras se analizan los documentos, en el apartado **Documents** irán clasificándose todos los archivos descargados según su extensión.



12. En la parte de **MetadataSummary**, aparecerá un resumen o clasificación de los metadatos encontrados en los documentos de acuerdo con su tipo (nombres de usuarios, impresoras, software, e-mail, sistemas operativos, passwords, etc.).



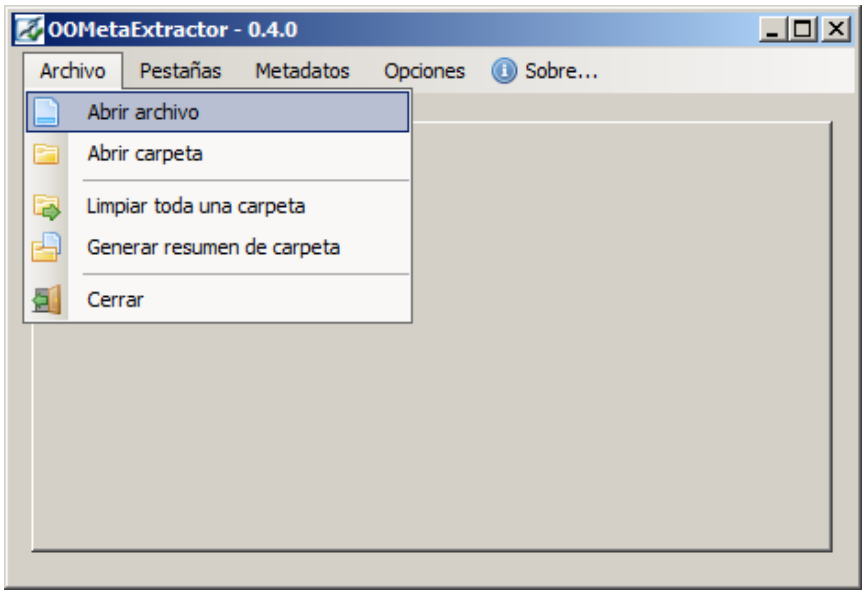
13. Una opción atractiva es hacer clic con el botón secundario del mouse sobre el apartado Metadata, lo cual presenta la opción Export, que realizará la exportación de los metadatos a otro documento.

V. Herramienta para la eliminación de metadatos OOExtractor

Este programa sirve para extraer y eliminar los metadatos de archivos generados por **Open Office** (*.odt, *.ods, *.odg, *.odp, *.sxw). **DESCARGA A TRAVÉS DE: http://oometaextractor.codeplex.com/releases/view/26811**

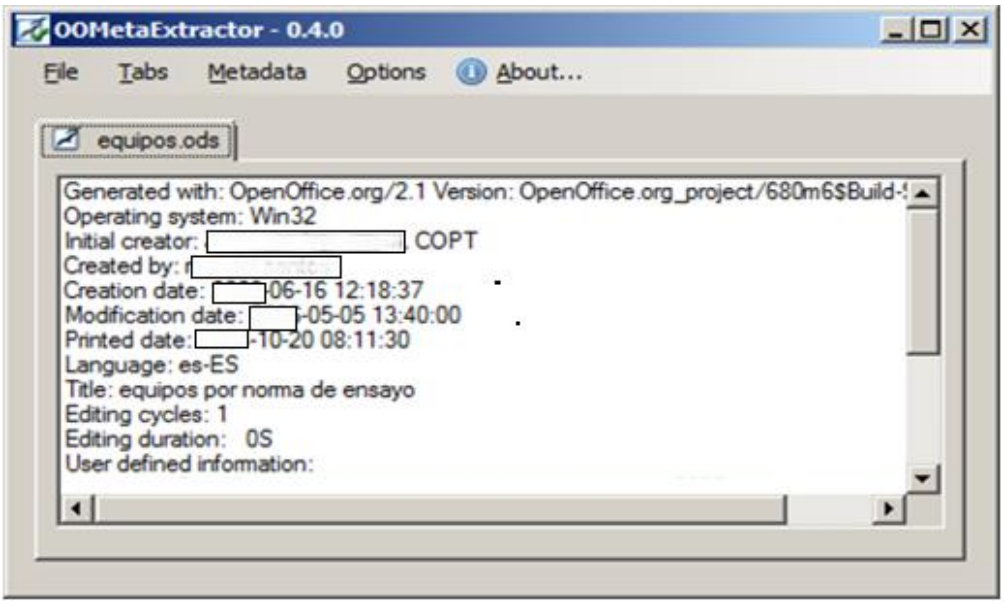
Borrado de metadatos de un archivo

1. Primero se hace clic en la pestaña **Archivo-Abrir Archivo.**



2. Se selecciona el archivo por analizar.

3. Seguidamente, se abrirá una nueva pestaña con el nombre del archivo que contiene los metadatos encontrados en éste.



4. Para el borrado de los metadatos de este archivo, en la pestaña Metadatos se selecciona la opción **Cleanmetadata in thistab**, lo cual borrará los metadatos del archivo cuya ventana esté activa.

5. Se selecciona la pestaña.

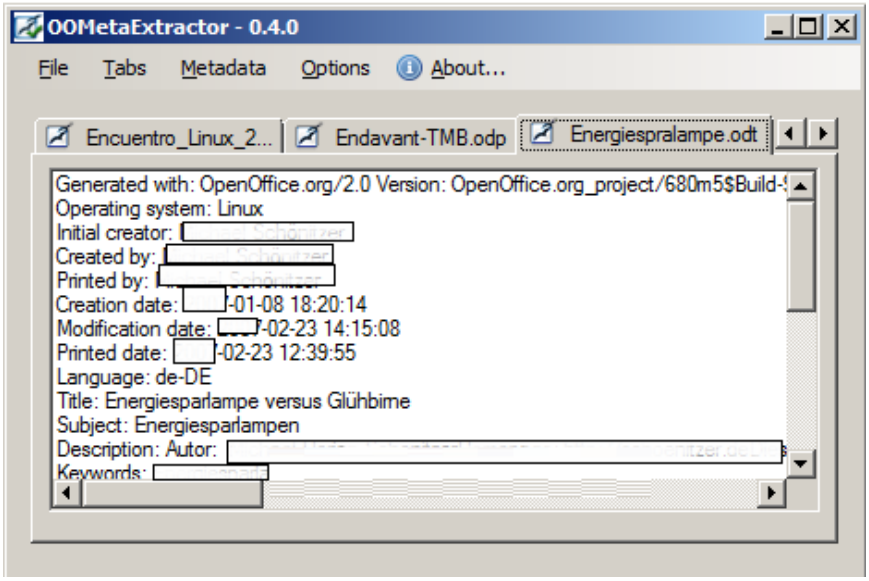
a) <u>Borrado de metadatos de una carpeta completa</u>

OOMetaExtractor ofrece la facilidad de realizar el borrado de metadatos de una carpeta completa, solucionando así el de realizarlo archivo por archivo.

1. Se hace clic en la pestaña **Abrir carpeta (**hay que recordar que solo se abrirán aquellos archivos creados con Open Office)**.**

2. La aplicación permitirá seleccionar la carpeta deseada.

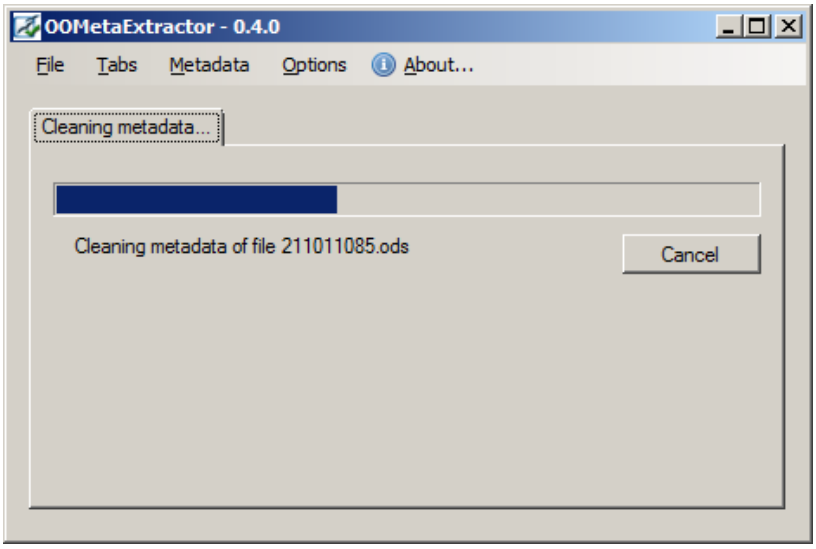
3. Seguidamente, se crearán pestañas por cada uno de las aplicaciones OpenOffice contenidas en la carpeta, cada pestaña muestra los metadatos contenidos en cada archivo.



4. Se puede realizar el borrado archivo por archivo, en caso de encontrar más de diez archivos en un mismo directorio se ofrecerá directamente la opción de eliminar los metadatos de todos los ficheros encontrados.

5. La opción Metadatos-Limpiar metadatos en todas las pestañas borra los metadatos de los ficheros abiertos en todas las pestañas.

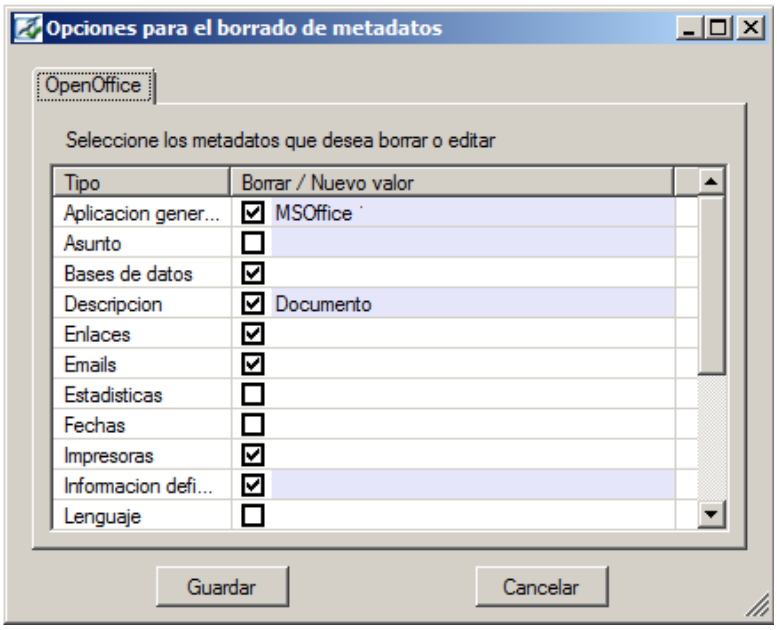
6. Se puede elegir también la opción **Limpiar toda una carpeta, lo** cual eliminará los metadatos de todos los archivos de Open Office que encuentre en la carpeta que se seleccionó.



En la pestaña **Archivo/Generar resumen de carpeta** se brinda la facilidad de poder generar un resumen en un archivo de texto “.txt” con la información más interesante de cada documento contenido en la carpeta seleccionada.

b) <u>Otras funcionalidades del menú de OOMetaExtractor</u>

- **Opciones de borrado de metadatos:** muestra una ventana donde se puede seleccionar los metadatos de los documentos de OpenOffice que se desean borrar. Aquellos valores que estén marcados con fondo azul permiten introducir o modificar el valor de la información encontrada.

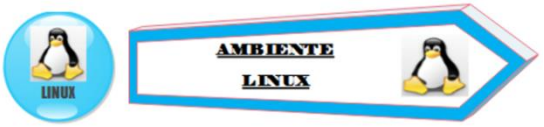


VI. Herramienta para la eliminación de metadatos Libextractor

DESCARGA A TRAVÉS DE: http://www.gnu.org/software/libextractor

DESCARGA A TRAVÉS DE: http://ftpmirror.gnu.org/libextractor/libextractor-0.5.23-w32.zip

VII. Herramienta para la eliminación de metadatos Metagoofil



DESCARGA A TRAVÉS DE: https://code.google.com/p/metagoofil/downloads/list

CAPÍTULO VI

CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

- El proyecto contó con los recursos necesarios para su desarrollo y con el apoyo de la universidad. Además, fue muy valioso el aporte de los profesionales de las instituciones, así como de especialistas en seguridad informática y seguridad de la información de cada institución, quienes permitieron y brindaron los espacios necesarios para el desarrollo del proyecto.

- La realización del proyecto pretende constituirse en una herramienta estratégica de gran ayuda, que permita generar conciencia de una problemática que ocurre y que puede afectar cualquier institución en la actualidad.

- Aprovechando las capacidades y conocimientos de expertos en manejo de entornos tecnológicos y en seguridad de la información, se logró dar a conocer la situación que se presenta en las instituciones y, con base en esto construir mecanismos de prevención y atención de temas asociados a la fuga de datos que se produce a través de metadatos.

- La propuesta metodológica desarrollada para atender el tema de fuga de datos que se produce a través de metadatos requiere de capacidades y conocimientos de personas para que puedan verdaderamente cumplir el fin de prevención, atención y protección acordes a los objetivos por los que se desarrolló el proyecto.

- El desarrollo de la investigación mostró una falta de conciencia a nivel institucional e individual de los riesgos relacionados con la fuga de información, razón por la que abordar este problema requiere una

combinación de consideraciones como: formación y concientización, el desarrollo de políticas a lo interno de cada institución y la aplicación de controles que prevengan este tipo de situaciones. Cada institución debe ser consiente de los riesgos y de los esfuerzos que se deben de realizar para reducirlos.

- La atención de esta problemática requiere de una tarea conjunta entre distintas áreas y personas a lo interno de las instituciones y un completo apoyo de parte de las autoridades correspondientes, posibilitándose con esto la comprensión, prevención y resolución de problemas relacionados a la fuga de datos.

- Es conocido que no se puede eliminar un riesgo completamente, cualquier institución está expuesta a que le ocurra un incidente, por lo que resulta fundamental que los esfuerzos vayan dirigidos a estrategias y acciones ya probadas y que generen confianza a la organización y que, en caso de ocurrir una situación, esta no tenga consecuencias mayores dentro de las organizaciones.
- Las instituciones públicas no cuentan con políticas de educación para el usuario respecto al uso correcto de la información, siendo necesario a lo interno que se consideren acciones para mejorar esta situación, que permita realizar un manejo adecuado de la información.
- A nivel nacional e internacional, no existe normativa o legislación asociada al tema de la fuga de datos originada por metadatos.
- Es necesario que se realicen procesos de evaluación de riesgo de pérdida de la información o fuga de datos, porque solo de esta forma se podrá determinar realmente las consecuencias que vaya a tener en una institución si llegará a materializarse.
- Según los resultados obtenidos de los instrumentos aplicados, no se atiende en las instituciones. Por esta razón, resulta prioritario enfocar los esfuerzos en realizar tareas como limpieza de metadatos a documentos de

acceso público. Además, se evidencia una brecha de seguridad que puede ser utilizada por terceros para obtener información.

- La información recopilada permite determinar que las instituciones están realizando esfuerzos para efectuar un adecuado tratamiento a la información y, de esta forma, evitar que incidentes por fuga de información tengan un impacto negativo. No obstante, y a pesar de lo trascendental que se considera el tema a nivel mundial, otras no lo atienden con la importancia que debe tener o no han buscado los mecanismos necesarios para prevenir y reducir los efectos que pudiera causar.

- Los resultados anteriores dejan en evidencia situaciones como:

- Falta de capacitación y concientización del personal encargado de atender el tema de seguridad informática y seguridad de la información en algunas áreas.
- Las instituciones están completamente expuestas a que se produzca una fuga de datos a través de metadatos contenidos en documentos de acceso público.
- Las fugas de datos a nivel general por aspectos no asociados a metadatos aún no se atienden adecuadamente, posiblemente porque se carece de los recursos (personales, económicos y equipos) destinados para este fin. Al no atenderse el tema de fuga de datos que pueda producirse a través de metadatos, están evidenciando falencias que pueden generar consecuencias (reputacionales, legales, económicas) a nivel institucional.

- Debe existir un mayor compromiso por parte de los encargados del departamento de informática para que involucren a todo el personal a lo interno en los proyectos de prevención y protección de datos que se realicen.

- Es necesario que exista profesionales con capacidades y conocimientos en el área de seguridad informática y seguridad de la información que pueda realizar trabajos de investigación y, con esto, se puedan desarrollar e

implementar estrategias que propicien mejoras en el área de seguridad informática.

- La realización del proyecto pretende constituirse en una herramienta estratégica de gran ayuda, que permita generar conciencia de una problemática que ocurre y que puede afectar cualquier institución en la actualidad.

- Al concienciar y fortalecer el conocimiento de los profesionales de seguridad sobre el campo de la seguridad informática y el manejo de metadatos, se podrá disminuir las vulnerabilidades y amenazas a las que se exponen las personas al publicar documentos de acceso general sin utilizar las medidas y mecanismos de prevención correctos.

- La formación en esta área mejorará la percepción que se tiene de la seguridad en las instituciones y los departamentos de informática, dado que este proyecto responde a las necesidades básicas y comunes que tienen los usuarios de acceso a documentos que usan herramientas computacionales.

6.2 Recomendaciones

- Es necesario que se realice y se apliquen medidas de seguridad, que permitan la eliminación y existencia de metadatos en documentos de acceso público y en general de todo lo relacionado al tema de fuga de datos. Esto porque se evidenció la poca o nula regulación que existe a nivel nacional e internacional relacionada con esta temática, además de lo fácil que resulta irrespetar las prohibiciones y las pocas directrices de seguridad informática que existen para tender este tema.
- Debe existir un mayor seguimiento y compromiso por parte de las autoridades que tienen a su cargo el desarrollo de normativa y, principalmente, los que tienen la labor de velar porque se le dé un uso adecuado a los recursos que posee la institución. También se deberían de

propiciar espacios de aprendizaje y concientización, en los cuales se elaboren los procedimientos correctos para la limpieza y extracción de metadatos y así se logren desarrollar los conocimientos que permitan resaltar la importancia de prevenir la ocurrencia de una fuga de datos, así como de seguridad informática, independientemente del área en que se aplique y del tema que atienda.

- La institución cuenta con profesionales titulados y capacitados en los departamentos de informática, por lo que resulta necesario que se involucren y generen experiencias, que permitan un nivel de seguridad mejor, así como un control adecuado en el acceso y utilización de los recursos institucionales.
- Tanto los profesionales de seguridad informática, así como los altos jerarcas en las instituciones deberán generar espacios en los cuales los trabajadores y el personal aprendan y desarrollen sus conocimientos en estas temáticas, permitiendo así que se investiguen y den solución a vulnerabilidades que existan, pero además que se les permita ir apropiándose de conocimiento y genere en ellos una cultura de seguridad informática y de protección de datos.
- Se debe elaborar y aplicar una reglamentación de seguridad informática, en la que se consideren desde aspectos generales que minimicen el riesgo de que se produzca una fuga de información, así como específicos que plasmen consideraciones necesarias para realizar una limpieza correcta de metadatos contenidos en documentos. Además, esta reglamentación debe actualizarse, explicarse y darse a conocer de ser posible a todos los usuarios (clientes, proveedores, personal), con la finalidad de ir formando y educando a la población en cuanto al uso y aplicación de mejores prácticas de seguridad de la información que contribuyan en prevenir la fuga de datos.

- Tanto los profesionales de seguridad de las instituciones, así como el personal técnico deberían informarse, investigar y profundizar los

conocimientos asociados a esta área, como parte de su desarrollo profesional y personal, esto porque a diario se dan a conocer nuevas técnicas, métodos y estrategias que se utilizan para vulnerar equipos, produciendo amenazas o riesgos en los lugares donde utilicen equipos computacionales. De esta forma, se podrían implementar acciones correctivas en los lugares de trabajo.

- Es importante que los encargados de la seguridad en las instituciones envíen, al menos una vez al mes, algún tipo de informe, boletín y noticia mediante una presentación audiovisual (menor a 5 minutos), un documento impreso o fotocopiado (máximo una hoja), o un correo electrónico, de algún tema relacionado a la seguridad informática y que genere en las personas que lo observan un interés por este tema y una cultura de protección de la información.

- El empleo de herramientas (DLP, filtrados de contenido, etc.) para evitar la fuga de información puede ayudar a limitar el riesgo de exposición de datos, con lo cual se limita el número de personas que puede verse afectada o la información que pueda ser comprometida, sin embargo, el personal de la institución, además de utilizar las herramientas y tecnologías apropiadas para atender este tipo de situaciones, también necesitan ser capacitados en la gestión de los riesgos asociados a la fuga de información, recordando que ninguna tecnología trabaja de manera efectiva de forma aislada y que se necesita de un enfoque coordinado (persona, conocimiento y tecnología) para poder lograr los resultados esperados.

Es importante enfatizar en aspectos como capacitación y concienciación del personal de la entidad como una medida preventiva para atender esta situación, así como que se asignen los recursos necesarios que permitan que se atienda adecuadamente.

- A pesar de que existe algún tipo de conocimiento por parte de personeros de seguridad informática y seguridad de la información referente a los

metadatos y los riesgos que pueden ocasionar, dentro de las instituciones muy poco o casi nada es lo que se realiza para atender esta situación. Esto demuestra que, a pesar de los esfuerzos como inversiones de recursos económicos, profesionales, capacitaciones, procesos de concientización, entre otros, existen vulnerabilidades que amenazan a las instituciones y generan un riesgo que debe en primera instancia darse a conocer y posterior a esto atenderse del mismo modo que otros escenarios en los cuales pueda existir fuga de información.

- El abordaje de incidentes ocasionados por fugas de información debe realizarse por profesionales, que tengan la capacidad de atender de manera integral cualquier situación.
- Ante la sospecha de que una situación irregular se puede estar presentado, se debe notificar al superior inmediato o en su defecto al área de respuesta a incidentes, ya que son quienes tomen las mejores decisiones para atender este tipo de incidentes. Cabe recordar, además, que una comunicación oportuna indudablemente minimizaría el impacto que pueda tener este tipo de situaciones.
- Existen otras actividades (modificación de parámetros y ajustes de seguridad por personas sin autorización, utilización de dispositivos móviles en ambientes de trabajo sin algún tipo de control o regulación, uso de correo institucional para propósitos ajenos a sus labores, uso de equipos de cómputo o dispositivos de almacenamiento institucionales para propósitos personales y viceversa, entre otros) que aunque no están relacionadas directamente con la fuga de datos que pueda producirse a través de metadatos contenidos en documentos de acceso público, ocurren comúnmente y aumentan el riesgo de que ocurra una fuga de información, lo cual repercute directamente en la seguridad de los usuarios finales, y acarrea consecuencias para la institución.
- Aspectos asociados a buenas prácticas de seguridad informática, como aplicación de defensa en profundidad, mínima superficie de exposición y menor privilegio posible se deberían considerar y serían de mucha utilidad

para aquellos que participen en labores de aseguramiento e implementación de controles de seguridad de la información, del mismo modo que una adecuada gestión al asignar perfiles y roles dentro de las instituciones.

- Es necesario que las instituciones presupuesten y destinen anualmente los recursos necesarios, que le permitan ir mejorando sus capacidades técnicas, de recurso humano, equipo e infraestructura, garantizar el adecuado abordaje de esta y muchas otras problemáticas que puedan surgir y que puedan limitar el funcionamiento y la operación o hasta producir consecuencias (legales, reputacionales o financieras). Además, a manera de mejora continua es prioritario que como instituciones puedan ir desarrollándose y creciendo según las necesidades y avances de nuevas tecnologías si así lo requieren.

- Se debe revisar la documentación (políticas, normativas, procedimientos) al menos una vez al año, con el objetivo de mantener vigentes estos instrumentos, pero también, para asegurarse de que su aplicación permita que los niveles de riesgo identificados sean los aceptados.

- Es necesario el desarrollo de procedimientos que permitan la atención de la fuga de datos que se produce a través de metadatos. Aunado a esto, debe realizarse una revisión y limpieza de metadatos de documentos de acceso público, con el fin de evitar que información adicional (metadatos) pueda producir situaciones de fuga de información. Para atender este tipo de actividades, la opción de automatización del proceso podría hacer eficiente la labor, e independizar la seguridad del quehacer del usuario, de modo que el proceso se lleve a cabo de modo correcto independientemente de las labores que pudieran entorpecerlo diariamente.

- Se recomienda realizar la limpieza de metadatos, prioritariamente en actividades y en los procesos que se determinaron como sensibles y que

tengan un mayor impacto para la institución, y de ahí ir avanzando según el nivel de criticidad hasta atender toda la organización.

- Se debe dar a conocer y concientizar dentro de las instituciones la problemática asociada a la fuga de datos que se puede producir por metadatos, para que así se inicie con el desarrollo de hábitos que prevengan este tipo de situaciones o se asignen los recursos necesarios para su atención.

- Los lineamientos de seguridad reglamentados y autorizados para la eliminación y borrado de metadatos que se vayan a utilizar se deben aplicar en todas las áreas de la institución y deberán ser revisados al menos una vez al año, para verificar su funcionamiento y como parte de un proceso normal de mejora continua.

CAPÍTULO VII

TRABAJOS A FUTURO

- Los datos representan uno de los activos más valiosos que posee una institución, por lo que deben asegurarse dentro de las instituciones y hacer un uso eficiente y responsable de estos.
- Las instituciones deben trabajar en el desarrollo de un proceso o herramientas que permita atender el tema de la fuga de datos que se produce a través de metadatos, ya sea asignando personal o realizándolo de forma automatizada, para que así se realice permanentemente y con esto evitar posibles riesgos asociados a la fuga de datos.
- La evolución, el desarrollo y el uso de nuevos entornos tecnológicos (computación en la nube, internet de las cosas) traen consigo desconocidos y novedosos escenarios de riesgo que deberán ser atendidos y en los cuales los incidentes por fuga de datos tendrán que considerarse.
- La metodología desarrollada para atender el tema de fuga de datos producida a través de metadatos requiere de capacidades y conocimientos de personas para que puedan verdaderamente cumplir el fin de prevención, atención y protección acordes con los objetivos por los cuales se desarrolló el proyecto.
- Las instituciones deben potenciar de forma continua la evolución de las capacidades y aptitudes de los profesionales que atiendan ciberseguridad con el fin de atender un panorama cada vez más sofisticado de amenazas y riesgos que pueden afectarlos.
- De la mano con la existencia de policías y lineamientos que prevengan la ocurrencia de fuga de datos por metadatos a lo interno de las instituciones, existe un aspecto que reviste de importancia y que debe considerarse. Se basa en el hecho de que es igual de importante que se desarrolle una política, normativa o procedimiento, a que los conozca todo el personal dentro de la

institución, y que se ponga en práctica, por lo que los esfuerzos para divulgar, culturizar y dar a conocer un mecanismo o control desarrollado internamente debe responder a un objetivo coordinado que se proyecte desde la estructura más alta de la institución hasta todo el personal, proveedores y colaboradores.

- Una comunicación asertiva y un seguimiento del cumplimiento son aspectos fundamentales para garantizar un beneficio total de lo que se quiere y por lo que se han dedicados esfuerzos y recursos en su desarrollo.
- Es de vital importancia que durante cada proceso de concientización y de arraigo de hábitos en seguridad estos sean reforzados constantemente en todo el personal. Así la responsabilidad de la protección de cualesquiera de los entornos institucionales no solo se delega en los profesionales de seguridad y en los personeros de tecnologías, sino que se convertirá en una labor colaborativa de todos a lo interno de la organización, eso sí, con roles y responsabilidades claramente definidos y comunicados.

CAPÍTULO VIII

REFLEXIONES FINALES

- El desarrollo de la investigación mostró una falta de conciencia a nivel institucional e individual de los riesgos relacionados con la fuga de información, razón por la que abordar este problema requiere una combinación de consideraciones como: formación y concientización, el desarrollo de políticas a lo interno de cada institución y la aplicación de controles que prevengan este tipo de situaciones. Cada institución debe ser consciente de los riesgos y de los esfuerzos que se deben de realizar para reducirlos.
- A nivel nacional e internacional no existe normativa o legislación asociada al tema de fuga de datos originada por metadatos. La regulación existente básicamente se enfoca en la protección de datos personales, las instituciones que tratan de atender la prevención de fuga de datos lo realizan a nivel general, y describen mayoritariamente usos y capacidades de tecnologías, pero no enfocadas directamente ni parcialmente en la prevención de fuga de datos que se origina por metadatos. Por ello se recomienda que se realicen esfuerzos por dar a conocer esta problemática, que atiende este trabajo de investigación, a las instituciones encargadas de generar normativas y legislación en temas de seguridad informática y seguridad de la información.
- Las estrategias y buenas prácticas, que se dieron a conocer y que pretenden corregir y atender aspectos que no son considerados actualmente en las instituciones públicas y la comunidad en general, serán efectivas si se adopta el proyecto como parte fundamental de una correcta formación en el área que atiende la protección de los datos, fuga de información y el uso correcto de la tecnología.

REFERENCIAS

Alvarez-Gayou, J. (2003). Como hacer investigación cualitativa: Fundamentos y Metodología. (1era edición). México: Editorial Paidós Mexicana S.A.

Ander-Egg, E. y Aguilar, M. (2005) Cómo elaborar un proyecto. Guía para diseñar proyectos sociales y culturales, (18 edición). Buenos Aires, Argentina: LUMEN/HVMANITAS

Aranda, G. (28 de octubre de 2013). La NSA espió 60 millones de llamadas telefónicas en España en solo un mes. Recuperado de http://rsocial.elmundo.orbyt.es/epaper/xml_epaper/El%20Mundo/28_10_2013/pla_11014_Madrid/xml_arts/art_18984645.xml?SHARE=6C23C0F29C6C4F158F7CA6264B48630506AD61DD69EAC95847800EEAA0DD486EF7B4E5C83F4B54F0332949BD1E440A788F85104DA6A34116F0BF2991CF6C57D7F3103F9F8955D6CB5C2E20F19F56E1BFC1643039A79E22E58E3C823D77EC1368

Berts (2006) Gestión de proyectos educativos. (Primera edición). Perú: Editorial fondo Lima.

Borghello, C. (2001) Seguridad Informática - Implicancias e implementación. Recuperado el miércoles 14 de Marzo de 2016, de http://www.segu-info.com.ar/tesis/

Bortnik, S. (13 de abril de 2010) Qué es la fuga de información. Recuperado el 15 de febrero de 2016, de http://www.welivesecurity.com/la-es/2010/04/13/que-es-la-fuga-de-informacion/

Calvo, A. (s.f.) Fuga de información la mayor amenaza para la reputación corporativa. Recuperado el 15 de febrero de 2016, de http://www.redseguridad.com/opinion/articulos/fuga-de-informacion-la-mayor-amenaza-para-la-reputacion-corporativa

Cebrián, R. (15 de agosto de 2013) Fuga de información en empresas líderes en Data LossPrevention. Recuperado el 19 de febrero de 2016, de http://blog.elevenpaths.com/2013/08/fuga-de-informacion-en-empresas-lideres.html

Chema, A. (05 de noviembre de 2009) Esquema Nacional de Seguridad: Metadatos. Recuperado el 15 de febrero de 2016, de http://www.elladodelmal.com/2009/11/esquema-de-seguridad-nacional-metadatos.html

Chipchase, E. (2008) Los metadatos de marketing: riesgos y oportunidades. Recuperado el 11 de marzo de 2016, de https://hbr.org/2008/02/metadata-marketing-risks-and-o

Cisco (12 de marzo de 2014) Data Leakage Worldwide: Common Risks and Mistakes Employees Make. Recuperado el 15 de febrero de 2016, de http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/data-loss-prevention/white_paper_c11-499060.html

Cisco System Inc. (08 de febrero de 2008) Fuga de datos a nivel mundial: Riesgos y errores comunes de los empleados. Recuperado el 15 de febrero de 2016, de http://www.cisco.com/web/offer/em/pdfs_innovators/LATAM/data_mist_sp.pdf

cnnexpansion.com (9 de febrero 2016) ‘Hackers’ publican los datos de 20000 empleados del FBI. Recuperado el 22 de febrero de 2016, de http://www.cnnexpansion.com/economia/2016/02/09/hackers-publican-datos-de-20000-empleados-del-fbi

Cordero, C. (13 de noviembre de 2014) Fuga de datos impacta marcas, pero empresas carecen de tecnología para enfrentar crisis de imagen. Recuperado el 15 de febrero de 2016, de

http://www.elfinancierocr.com/tecnologia/Deloitte-reputacion-redes_sociales_0_628137189.html

El país.com (05 de junio de 2015) Un ciberataque afecta a millones de funcionarios de Estados Unidos. Recuperado el 15 de febrero de 2016, de http://internacional.elpais.com/internacional/2015/06/05/actualidad/1433458231_191963.html

Rambla, J; Blázquez, J; Alonso (2011). Esquema Nacional de Seguridad con Microsoft, Microsoft Ibérica S.R.L. Madrid, España. Informatica64

Esquivel, F. (2013) Lineamientos para diseñar un estado de la cuestión en investigación educativa. San José, Costa Rica: Escuela de Trabajo Social. Universidad de Costa Rica

ESET (2011) Fuga de información: ¿una amenaza pasajera? Recuperado el 15 de febrero de 2016, de http://www.eset-la.com/pdf/prensa/informe/fuga_de_informacion.pdf

ESET (2016) Security Everywhere. Cobb Stephen Senior Security Researcher. Recuperado el 15 de febrero de 2016, de http://www.welivesecurity.com/wp-content/uploads/2016/01/Tendencias_2016_insecurity_everywhere_eset.pdf

Felten, E. (23 de Agosto de 2013) Declaration of professor Edward w. Felten.Recuperado el 10 de marzo de 2016, de http://ia601803.us.archive.org/22/items/gov.uscourts.nysd.413072/gov.uscourts.nysd.413072.27.0.pdf

Fisher, D. (13 de marzo de 2014) Estudio muestra lo altamente sensibles que son los metadatos en los teléfonos. Recuperado el 19 de febrero de 2016, de https://threatpost.com/study-shows-phone-metadata-is-highly-sensitive/104767/

Galeano, M.E. (2004) “Diseño de proyectos en la investigación cualitativa”. Fondo Medellín, Colombia: Editorial Universidad EAFIT

Gartner, Inc. y / o sus afiliados. (2017). Cuadrante Mágico 2017 de Gartner para prevención contra la pérdida de datos empresariales. Recuperado el 07 de Marzo de 2017, de https://www.gartner.com/doc/reprints?id=1-3TOGM5S&ct=170216&st=sb

González, D; Martínez, A; Pérez, T; Zárate, J. (2010) Modelo de seguridad para la prevención de pérdida de datos en las organizaciones. Tesina para obtener el título de Licenciado en Ciencias de la Informática, Instituto Politécnico Nacional, México, D.F.

Gonzalo, M. (23 de octubre de 2013) Qué son tus metadatos y por qué pueden ser tan importantes como el contenido de tu email. Recuperado el 10 de Marzo de 2016, de http://www.eldiario.es/turing/vigilancia_y_privacidad/metadatos-pueden-importantes-contenido-email_0_190731401.html

Gutiérrez, C. (08 de enero de 2015) 10 años de fuga de información: conoce los incidentes para no repetir la historia. Recuperado el 19 de febrero de 2016, de http://www.welivesecurity.com/la-es/2015/01/08/10-anos-fuga-de-informacion/

Hernández, R., Fernández, C. & Baptista, P (2006). Metodología de la investigación, 5ª edición. Distrito Federal, México: McGraw-Hill.

INCIBE (20 de julio de 2015) Cómo gestionar una fuga de información. Una guía de aproximación para el empresario. Recuperado el 15 de febrero de 2016, de https://www.incibe.es/extfrontinteco/img/File/empresas/guias/Guia_fuga_informacion/gestion_fuga_informacion.pdf

INCIBE (20 de julio de 2015) Cómo gestionar una fuga de información. Recuperado el 15 de febrero de 2016, de https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_gestion_fuga_informacion_0.pdf

INCIBE (18 de enero de 2017) ¿Estás preparado para hacer frente a una fuga de datos? Recuperado el 28 de marzo de 2017, de https://www.incibe.es/protege-tu-empresa/blog/estas-preparado-hacer-frente-fuga-datos

Smilkov, D. JagdishD. Hidalgo, C. (06 de julio de 2013). Recuperado el 15 de febrero de 2016, de https://immersion.media.mit.edu/

INCIBE (27 de enero de 2016) Protección de la información. Recuperado el 15 de febrero de 2016, de https://www.incibe.es/protege-tu-empresa/que-te-interesa/proteccion-informacion

INTECO-CERT (2012) Gestión de fuga de información. Recuperado el 15 de febrero de 2016, de https://www.incibe.es/extfrontinteco/img/File/empresas/dosieres/protege_tu_informacion/guia_gestion_fuga_informacion.pdf

ISACA (2010) Prevención de fuga de datos. 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008 EE.UU. www.isaca.org

Latorre, A. (2005) La investigación-acción. Barcelona, España: Editorial Grao. Tercera edición

Luiz, M; Borboa, M; Rodríguez, J. (2013) El enfoque mixto de investigación en los estudios fiscales. Tlatemoani, Revista Académica de Investigación. Editada por Eumed.net. España

Martínez, L. (02 de febrero de 2014) Base de Datos. Recuperado el miércoles 14 de marzo de 2016, de http://ramirezmartinezluis.blogspot.com/2014/02/normal-0-21-false-false-false-es-mx-x.html

Pagnotta, A. (10 de febrero de 2016) ¿Sabes que es la Haxposición? Conoce a esta amenaza emergente. Recuperado el 15 de febrero de 2016, de http://www.welivesecurity.com/la-es/2016/02/10/que-es-haxposicion-amenaza-emergente/

Pérez, A. (2009). Guía metodológica para anteproyectos de investigación. Caracas: Fondo Editorial de la Universidad Pedagógica Experimental Libertador (FEDUPEL)

Pérez, N. (julio de 2013) Factibilidad Técnica y Operacional. Recuperado el 2 de Febrero de 2016, de https://sites.google.com/site/gerenciadeproyectouma/semestre-i/factibilidad-tecnica-y-operacional

Ponce, M. (marzo de 2002) Guía para realizar estudios de factibilidad y pertenencia de programas Educativos. Recuperado el 2 de febrero de 2016, de http://www.uaeh.edu.mx/planeacion/images/pdf/1_guia_factibilidad.pdf

Pumarino, A. (5 de junio de 2006) ¿Qué es la seguridad informática? Recuperado el jueves 14 de marzo de 2016, de http://pumarino.blogspot.com/2006/06/qu-es-la-seguridad-informtica.html

PWC (02 de Junio de 2015) TechnicalReport, Information Security Breaches Survey Recuperado el lunes 4 de marzo de 2016, de https://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-digital.pdf

RAE (2016) Información. Recuperado el lunes 4 de Marzo de 2016, de http://dle.rae.es/?id=LXrOqrN

Ruiz, C. (12 de Junio de 2014) 75% de las empresas de Costa Rica sufrieron al menos un incidente de seguridad informática en 2013. Recuperado el 15 de febrero de 2016, de http://www.nacion.com/tecnologia/informatica/empresas-sufrieron-incidente-inseguridad-informatica_0_1420258093.html

Sapag, C; Nassir (2007) Proyectos de inversión, formulación y evaluación. (Primera Edición) Editorial Prentice Hall.

Senn, J. (1993) Sistemas de Información para la Administración. México, Grupo Editorial Iberoamericano. 3a. Edición

Senso, J.; Piñero, A. (agosto de 2003) El concepto de metadato. Algo más que descripción de recursos electrónicos. Recuperado el viernes 25 de Febrero de 2016, de http://www.scielo.br/pdf/ci/v32n2/17038.pdf

Symantec (25 de noviembre de 2015) Data Loss Prevention is not detecting file metadata. Recuperado el 16 de febrero de 2018, de https://support.symantec.com/en_US/article.TECH233582.html

Welivesecurity. (06 de julio de 2016) Conoce tus puntos débiles y evita la fuga de datos. Recuperado el 12 de agosto de 2016, de https://www.welivesecurity.com/la-es/2016/07/06/puntos-debiles-evita-fuga-de-datos/

CAPÍTULO IX

ANEXOS

ANEXO 1

Cuestionario dirigido al personal de la Institución

Marzo 2017.

Nota: La información obtenida será confidencial y se utilizará únicamente para fines educativos.

1 ¿Qué es la fuga de información?

_____

_____

2 Según su criterio, ¿cuál es el motivador principal para que se dé una fuga de información?

( ) Origen interno

( ) Origen externo

( ) Ambas

3 Indique si Recursos Humanos en su institución cuenta con políticas de educación a los usuarios respecto al uso de la información

( ) No tiene

( ) Piensa hacerlo

( ) En desarrollo

( ) Aplica mensualmente / trimestralmente

( ) Aplica anualmente

4 De las siguientes herramientas ordene en orden de prioridad (siendo 1 la más importante) aquellas soluciones que usted relaciona con la protección contra robo de información:

( ) Antivirus

( ) IPS de Red

( ) Firewall

( ) Antispam

( ) Filtros de Contenido

( ) Otros indique:_____

5 ¿Aplica su organización procesos de evaluación de riesgo de pérdida de la información?

( ) Sí

( ) No

6 El acceso a la información en la institución está según su criterio acorde con los privilegios y necesidades que debería tener cada área y persona en la institución

( ) Sí

( ) No

7 ¿Cuáles considera serían los impactos más severos que tendría una fuga de datos en su institución? enumérelos de acuerdo con su importancia (siendo 1 el mayor impacto).

( ) Daño reputacional (imagen)

( ) Sanciones económicas

( ) Perdidas de clientes

( ) Consecuencia legales

( ) Interrupción en la continuidad de los servicios

( ) Otra _____

8 ¿Cuáles serían las causas que considera más relevantes y que podrían propiciar una fuga de datos en la institución en la que labora?

( ) Empleados descontentos

( ) Errores y fallas de los empleados

( ) Falta de políticas

( ) Poca concientización y capacitación

( ) Formación profesional débil

9 De los siguientes motivos internos que podrían producir una fuga de datos, ¿Cuál considera el aspecto principal que podría producirlos?

( ) Por errores inadvertidos (desconocimiento, error)

( ) Por errores voluntarios (descontento, venganza, beneficio económico, daño imagen, competencia)

10De los siguientes motivos internos que podrían producir una fuga de datos, seleccione el que considera más importante en cada categoría.

Errores inadvertidos

( ) Desconocimiento

( ) Error

Errores voluntarios

( ) Descontento

( ) Venganza

( ) Beneficio económico

( ) Daño imagen

( ) Competencia

11 ¿Cuál (es) motivos externos considera podrían producir una fuga de datos en su institución?

( ) Organizaciones criminales

( ) Activistas

( ) Beneficios económicos

( ) Fines extorsivos

( ) Daño a la imagen

( ) Vulnerabilidades en software

12 A nivel organizacional, ¿qué factor considera podría causar una fuga de datos?, Enumérelos de acuerdo con su importancia (siendo 1 el más importante).

( ) Falta de clasificación de la información

( ) Falta de conocimiento y formación

( ) Ausencia de procedimientos

( ) Ausencia de conocimientos

( ) Ausencia de acuerdos de confidencialidad

13 A nivel administrativo ¿qué factor considera podría causar una fuga de datos?, Enumérelos de acuerdo con su importancia (siendo 1 el más importante).

( ) Código malicioso

( ) Acceso no autorizado

( ) Servicios de almacenamiento externos

( ) Tecnologías móviles y webs

14 ¿La falta de cuáles de los siguientes aspectos podrían propiciar que se dé fuga de información?

( ) Medidas de seguridad

( ) Procedimientos establecidos

( ) Herramientas y/o dispositivos

( ) Concientización y capacitación

( ) Clasificación de la información

15 ¿Cuál aspecto considera más común que falte en las organizaciones?, Enumérelos del 1 al 5 siendo 1 el más importante.

( ) Medidas de seguridad

( ) Procedimientos establecidos

( ) Herramientas y/o dispositivos

( ) Concientización y capacitación

( ) Clasificación de la información

16 De las siguientes normativas o estándares enumere según la prioridad su uso a nivel interno:

( ) Cobit 5

( ) PCI DSS

( ) Normas Técnicas de la Contraloría General de la República

( ) Familia ISO 27000

17 Existe una gestión de incidentes de seguridad en su empresa.

( ) Sí

( ) No

18 ¿Existen equipos y/o herramientas destinadas específicamente para prevenir la fuga de datos?

( ) Sí

( ) No

19 ¿Se capacita la personal de la institución en temas de prevención de fuga de datos?

( ) Sí

( ) No

20 ¿Con qué frecuencia se capacita la personal de la institución en temas de prevención de fuga de datos?

( ) Semanal

( ) Mensual

( ) Trimestral

( ) Semestral

( ) Anual

( ) Otra

21 ¿Conoce qué son los metadatos?

( ) Sí

( ) No

22 ¿Considera que se puede producir una fuga de información a través de metadatos?

( ) Sí

( ) No

23 En la institución en la que labora, ¿se realiza limpieza de metadatos a los documentos que se encuentran en sitios web o en repositorios de acceso público?

( ) Sí

( ) No

24 En la institución en la que labora, ¿existe un proceso formal para atender el tema de fuga de datos a través de metadatos?

( ) Sí

( ) No

25 ¿Considera prioritario que a nivel institucional se atienda adecuadamente el tema de fuga de datos, que podrían producirse a través de metadatos, contenidos en documentos que se encuentran en sitios web o en repositorios de acceso público?

( ) Sí

( ) No

Muchas gracias.

ANEXO 2

Cuestionario dirigido al personal de TI de la Institución

Marzo 2017.

Nota: La información obtenida será confidencial y se utilizará únicamente para fines educativos.

1 ¿Qué información considera se vería más afectada si se produce una fuga de datos en la institución en la que labora?

( ) Clientes

( ) Proveedores

( ) Personal de la institución

2 ¿Qué haría en caso de detectar una fuga de información?

( ) Comunicar a la jefatura

( ) Atender la situación

( ) Reportar el incidente a terceros

3 ¿Con qué periodicidad se supervisan las aplicaciones (software) instaladas en los dispositivos de trabajo en la institución?

( ) Nunca

( ) Una vez al mes

( ) Una vez cada trimestre

( ) Una vez al año

4 ¿Se regula el acceso/ ingreso de personal a distintas áreas de la institución?

( ) Sí

( ) No

5 ¿Con qué facilidad un empleado/colaborador de la institución podría tener acceso a equipos, dispositivos o información sensible a lo interno de la institución?

( ) Muy fácil

( ) Fácil

( ) Difícil

( ) Muy difícil

( ) Imposible

6 ¿Ha utilizado dispositivos personales para el almacenamiento de la información?

( ) Sí

( ) No

Si su respuesta es afirmativa, ¿con qué frecuencia?

( ) Solo una vez

( ) Pocas veces

( ) Constantemente

7 Existe alguna regulación con la utilización de dispositivos móviles personales en la institución.

( ) Sí

( ) No

8 ¿Cuáles dispositivos móviles considera son los más utilizados por los usuarios en la institución?

( ) Cámaras

( ) Teléfonos

( ) Tabletas

( ) Otros:_____

9 ¿Existen regulaciones con la creación, uso y almacenamiento de las contraseñas por parte del personal de la institución?

( ) Sí

( ) No

10 ¿Se capacita al personal de la institución en temas de gestión de contraseñas?

( ) Sí

( ) No

11 ¿Se permite a los usuarios modificar los parámetros y ajustes de seguridad en los equipos?

( ) Sí

( ) No

12 ¿Se han detectado incidentes de fuga de datos por la modificación de parámetros y ajustes de seguridad en los equipos de la institución?

( ) Sí

( ) No

13 ¿Cuál considera es la causa principal de que los usuarios modifiquen parámetros y ajustes de seguridad en sus equipos?

( ) Ingresar a sitios web no autorizados

( ) Instalar software

( ) Utilizar componentes de hardware

( ) Otros: _____

14 ¿Con qué frecuencia utiliza o ha utilizado el correo electrónico institucional para uso personal?

( ) Nunca

( ) Cierta periodicidad

( ) Siempre

( ) Constantemente

15 ¿Con qué frecuencia utiliza el correo personal para enviar información a clientes, proveedores, socios, compañeros de trabajo, otros?

( ) Nunca

( ) Cierta periodicidad

( ) Siempre

( ) Constantemente

16 ¿Con qué frecuencia utiliza o ha utilizado los equipos de cómputo institucionales para propósitos personales?

( ) Nunca

( ) Cierta periodicidad

( ) Siempre

( ) Constantemente

17 Enumere de acuerdo a su importancia (siendo 1 el más importante) que actividades considera son más frecuentes que se realicen en equipos institucionales

( ) Acceder a redes sociales

( ) Descargar contenido (música, fotos, vídeos)

( ) Juegos

( ) Almacenamiento externo o en la nube

( ) Otras

18 ¿Cuáles de los siguientes comportamientos se han detectado en la institución?

( ) Uso de aplicaciones no autorizadas

( ) Uso de correo personal en equipos institucionales

( ) Uso del equipo de trabajo para propósitos personales

( ) Alteración de parámetros de seguridad en equipos y dispositivos

( ) Compartir información institucional con personas ajenas a la institución

( ) Uso de equipos institucionales para actividades como compras en línea, pago de servicios, juegos, descargas de contenido.

( ) Revelar información a amigos y familiares.

19 ¿Existen políticas de seguridad o lineamientos específicos para atender el tema de la fuga de datos en la institución en que labora?

( ) Sí

( ) No

20 ¿Son de conocimiento y aplicación de toda la empresa?

( ) Sí

( ) No

21 ¿Se comparten dispositivos institucionales de trabajo entre compañeros?

( ) Sí

( ) No

22 ¿Cuáles dispositivos de trabajo considera común que se compartan entre compañeros a lo interno de la institución?

( ) USB

( ) Teléfonos celulares,

( ) Discos duros

( ) Cámaras fotográficas

( ) Otros:_____

23 ¿Se utilizan dispositivos institucionales para propósitos personales fuera de la institución?

( ) Una vez al día

( ) Una vez a la semana

( ) Algunas veces a la semana

( ) Algunas veces al mes

( ) Muchas veces al mes

( ) Nunca

24 ¿Se utilizan controles para evitar el acceso de personas no autorizadas a la institución?

( ) Sí

( ) No

25 ¿Se han registrado casos de personas no autorizados en la institución?

( ) Sí

( ) No

( ) No conozco

26 ¿Se ha valido de amigos para ingresar a lugares a los que no tiene permiso o privilegios para ingresar?

( ) Sí

( ) No

#27 ¿Transfiere o ha transferido información (datos) de un dispositivo de trabajo a un dispositivo personal?

( ) Una vez al día

( ) Una vez a la semana

( ) Algunas veces a la semana

( ) Algunas veces al mes

( ) Muchas veces al mes

( ) Nunca

#28 En la institución en la que labora, ¿se permite que dispositivos institucionales accedan a conexiones de red personales?

( ) Sí

( ) No

29 ¿Qué acciones se podrían considerar para la protección de los datos?

( ) Políticas de seguridad

( ) Líneas o protocolos de actuación

( ) Buenas practicas

( ) Formación y concientización

Muchas gracias.

ANEXO 3

Guía de observación

La siguiente tabla pretende obtener datos o aspectos que sean determinantes como requerimientos mínimos que debe contar la empresa a nivel técnico, así como el estado en el que se encuentran.

N°	Aspectos por considerar	Posee la institución		Estado en el que se encuentra				
		Si	No	Excelente	Bueno	Regular	Deficiente	
1.	Profesionales de Seguridad Informática/Seguridad de la Información							
2.	Mecanismos de clasificación de la información							
3.	Manejo de incidentes de seguridad							
4.	Política, normativas y procedimientos de seguridad de la información							
5.	Mecanismos que utilizan para							

	detectar la fuga de datos							
6.	El conocimiento de los usuarios de fuga de datos							
7.	El personal de la institución sabe de la existencia de metadatos.							
Observaciones: _____ _____ _____ ___								

Puntos por observar sobre el comportamiento y reacciones de los trabajadores, en las instituciones públicas de Costa Rica.

1 ¿Se regula el acceso/ ingreso de personal a distintas áreas de la institución?

2 ¿Con qué facilidad un empleado/colaborador de la institución podría tener acceso a equipos, dispositivos y/o información sensible a lo interno de la institución?

3 ¿Utiliza dispositivos personales para el almacenamiento de la información?

4 ¿Existe alguna regulación con la utilización de dispositivos móviles personales en la institución?

5 Uso del correo electrónico institucional para uso personal.

6 Uso del correo personal en equipo institucional.

7 ¿Se utilizan equipos institucionales para realizar algunas de las actividades siguientes?

( ) Acceder a redes sociales,

( ) Descargar contenido (música, fotos, videos)

( ) Juegos

( ) Almacenamiento externo o en la nube,

( ) Otras

8 Comportamientos

( ) Uso de aplicaciones no autorizadas

( ) Uso de correo personal en equipos institucionales

( ) Uso del equipo de trabajo para propósitos personales

( ) Alteración de parámetros de seguridad en equipos y dispositivos

( ) Compartir información institucional con personas ajenas a la institución

( ) Uso de equipos institucionales para actividades como compras en línea, pago de servicios, juegos, descargas de contenido.

( ) Revelar información a amigos y familiares.

9 ¿Se comparten dispositivos institucionales de trabajo entre compañeros?

( ) Sí

( ) No

10 ¿Cuáles dispositivos se emplean a lo interno de la institución?

( ) USB

( ) Teléfonos celulares,

( ) Discos duros

( ) Cámaras fotográficas

( ) Otros:_____

11 ¿Se utilizan controles para evitar el acceso de personas no autorizadas a la institución?

( ) Sí

( ) No

12 ¿Existen conexiones de red personales?

( ) Sí

( ) No

13 Al comentar de la existencia de metadatos al personal de la institución, que impresión se obtuvo.

Muchas gracias.