Propuesta metodológica para mitigar el riesgo de seguridad informática con el uso de técnicas OSINT.

Balcázar Lalangui, Mariela del Carmen

Departamento de Ciencias de la Computación

Carrera de Ingeniería de Sistemas e Informática

Trabajo de titulación, previo a la obtención del título de Ingeniera en Sistemas e Informática

Msc. Ron Egas, Mario Bernabe

16 de enero del 2020

Urkund Analysis Result

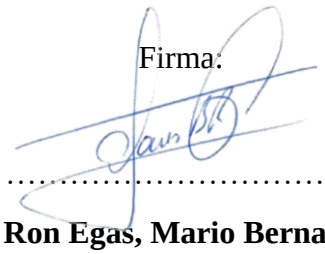
Analysed Document: Mariela Balcazar_Tesis_ESPE.docx (D62489523)
Submitted: 16/01/2020 19:06:00
Submitted By: jbolanos@difusion.com.mx
Significance: 10 %

Sources included in the report:

TT Alan Leiva final.docx (D57185675)
https://www.researchgate.net/publication/326599598_Modelo_de_gestion_de_riesgos_de_seguridad_de_la_informacion_para_PYMES_peruanas
https://www.slideshare.net/pierina224/gerencia-de-riesgos-semana-1-32473449
https://www.scribd.com/document/437236590/Foro-Unidad-2-Ender-Diaz
https://docplayer.es/3892711-Las-redes-sociales-como-fuentes-de-informacion-osint.html
https://www.powtoon.com/online-presentation/b5AuMm4w7GM/campana-riesgos-informaticos-1/?mode=Movie&locale=en
https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html
https://sites.google.com/site/convivenciacddigital/riegos-informaticos
https://link.springer.com/chapter/10.1007/978-3-319-47671-1_11
https://rua.ua.es/dspace/bitstream/10045/93271/1/Analisis_y_correlacion_entre_probabilidad_e_impacto_de_l_Santonja_Lillo_Juan.pdf
https://repository.ucatolica.edu.co/bitstream/10983/23377/1/Trabajo%20de%20Grado%20Seg.%20de%20la%20Informacion%20Final.pdf

Instances where selected sources appear:

Firma:



……

Ron Egas, Mario Bernabe

C. C. 1704229747

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN
CARRERA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

CERTIFICACIÓN

Certifico que el trabajo de titulación, "**Propuesta metodológica para mitigar el riesgo de seguridad informática con el uso de técnicas OSINT**" fue realizado por la señorita **Balcázar Lalangui, Mariela del Carmen** el cual ha sido revisado y analizado en su totalidad por la herramienta de verificación de similitud de contenido; por lo tanto cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, razón por la cual me permito acreditar y autorizar para que lo sustente públicamente.

Sangolquí, 16 de Enero del 2020

Firma:

.....

Ron Egas, Mario Bernabe
C. C. 1704229747

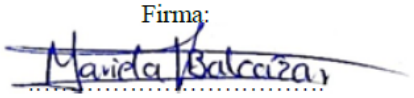
DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN
CARRERA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

RESPONSABILIDAD DE AUTORÍA

Yo, **Balcázar Lalangui, Mariela del Carmen**, con cédula de ciudadanía n° 1723663405, declaro que el contenido, ideas y criterios del trabajo de titulación**: Propuesta metodológica para mitigar el riesgo de seguridad informática con el uso de técnicas OSINT** es de mi autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos, y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Sangolquí, 16 de Enero del 2020

Firma:



Balcázar Lalangui, Mariela del Carmen
C.C. 1723663405

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN
CARRERA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

AUTORIZACIÓN DE PUBLICACIÓN

Yo, **Balcázar Lalangui, Mariela del Carmen**, con cédula de ciudadanía n° 1723663405, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación: **Propuesta metodológica para mitigar el riesgo de seguridad informática con el uso de técnicas OSINT** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi responsabilidad.

Sangolquí, 16 de Enero del 2020

Firma:

Balcázar Lalangui, Mariela del Carmen
C.C. 1723663405

Dedicatoria

Quisiera dedicar el esfuerzo de este trabajo a quienes han sido incondicionales y de indispensable ayuda durante el transcurso de mi vida estudiantil. A mis padres, ejemplos de constancia y dedicación. A mi familia que en todo momento me han apoyado por el apoyo, comprensión, paciencia y estar siempre a mi lado.

A todos aquellos que tuvieron fe en mí. A mis ingenieros que en las aulas durante el paso de mi vida estudiantil han sabido transmitirme la sabiduría necesaria para poder salir adelante y buscar un futuro en el cual espero este lleno de éxitos.

Este logro va por ustedes!

Agradecimiento

En primer lugar quiero agradecer a Dios por permitirme culminar una etapa tan importante dentro de mi vida académica. A mis padres por entregarme todo su apoyo, cariño y comprensión a lo largo de mi vida, por estar presentes en cada paso que eh sabido dar con sus bendiciones y su apoyo pude determinar mis prioridades para luchar por mis sueños, gracias mami por cada día acompañarme y ser mi apoyo físico y emocional siempre. A mi papi que confió siempre y sé que esperaba este logro gracias por confiar que yo lo cumpliría, por usted que siempre conto y puso su fe en mí, donde Dios lo tenga sé que está festejando este logro con todos los que me quieren.

Al Ing. Mario Ron, ya que sin su apoyo e interés no hubiese sido posible esta meta alcanzada. Y a todas aquellas personas que de alguna forma han contribuido con la realización de esta tesis.

A todos, muchas gracias

Índice de contenidos

Índice de tablas

Índice de figuras

Resumen

En la actualidad existen muchos ataques en la red que se deben al desconocimiento de técnicas en seguridad informática, el mayor riesgo para la información se encuentra en las redes sociales y en el acceso a la red en diferentes dispositivos, en los últimos años la información tiene mayor índice de vulnerabilidades por diferentes intereses, a pesar de la existencia de métodos para evitar amenazas y el robo de datos personales, estos métodos son desconocidos por los usuarios, lo que limita el uso correcto de la información y herramientas de protección, el análisis permite determinar el proceso de segregación y elección de la víctima.

Una de sus causas es desconocimiento de las técnicas utilizadas por OSINT, para ello al desarrollar una propuesta metodológica, basada en el análisis de riesgos de seguridad informática en OSINT, para minimizar el impacto de los ciberataques mediante métodos y técnicas de ciberseguridad y ciberdefensa donde se usara OCTAVE permite un plan de mitigación. Al diseñar la metodológica para el empleo ético de los métodos y técnicas de OSINT, tanto en ciberseguridad como en ciberdefensa, de esta manera aportar a las necesidades administrativas de las empresas, en la investigación se recomienda el proceso metodológico para el empleo ético de los métodos y técnicas de OSINT, tanto en ciberseguridad como en ciberdefensa, para conseguir habilidad en el empleo de las técnicas presentadas, para que se pueda establecer procesos seguros y evitar riesgos informáticos.

-Palabras clave:

- **OSINT**
- **OCTAVE**
- **MEHARI**

Abstract

Currently there are many attacks on the network that are due to ignorance of computer security techniques, the greatest risk for information is in social networks and in access to the network on different devices, in recent years information has higher index of vulnerabilities due to different interests, despite the existence of methods to avoid threats and the theft of personal data, these methods are unknown by users, which limits the correct use of information and protection tools, among other private information, the analysis makes it possible to determine the process of segregation and choice of the victim.

One of its causes is ignorance of the techniques used by OSINT, for this by developing a methodological proposal, based on the analysis of computer security risks in OSINT, to minimize the impact of cyberattacks using cybersecurity and cyber defense methods and techniques where using OCTAVE allows a mitigation plan. When designing the methodological for the ethical use of OSINT methods and techniques, both in cybersecurity and cyber defense, in this way to contribute to the administrative needs of companies, the research recommends the methodological process for the ethical use of methods and OSINT techniques, both in cybersecurity and cyberdefense, to achieve skill in the use of the techniques presented, so that safe processes can be established and computer risks avoided.

-Key words:

- **OSINT**
- **OCTAVE**
- **MEHARI**

Capítulo I

Introducción

Antecedentes

- En la actualidad existen muchos ataques en la red que se deben al desconocimiento de técnicas en seguridad informática. El mayor riesgo para la información se encuentra en las redes sociales y en el acceso a la red mediante diferentes dispositivos, con riesgos como suplantación de identidad mediante técnicas de Ingeniería Social y otros ataques que en la actualidad son considerados como delitos informáticos en algunos países, pero en otros no se encuentran tipificados; además no existe una práctica adecuada en el uso de la tecnología vigente para brindar seguridad al usuario en el manejo y administración de sus datos.
- En los últimos años se cuenta con mucha información en la red, que puede ser vulnerada por diferentes intereses, a pesar de la existencia de métodos para evitar la vulnerabilidad y el robo de datos personales. Muchos de estos métodos son desconocidos por los usuarios, lo que limita el uso correcto de la información, ya que no existe un análisis del tipo de ataque que puede darse y cuál sería el método para poder combatirlo. Es importante tener un análisis del rastro que deja el ataque para poder vulnerar los datos de la víctima y mediante el mismo proceso, pero de forma inversa mitigar ese ataque. El uso de la Inteligencia de Fuentes Abiertas (OSINT) permite actuar contra un ciberataque y activar ciberdefensa (Senekal & Kotzé, 2019).

Planteamiento del problema

- En la actualidad existe temor en el acceso a Internet por desconocimiento en el uso de la cantidad de información que se puede encontrar. Los usuarios toman riesgos al usar redes

sociales, compras online, entre otros aspectos en ámbitos como economía, educación, medicina, tecnología entre otros, pero al tener este acceso, los usuarios pueden ser sujetos de ataques de Ingeniería Social a su propia información privada, que es el tipo de ataque que se presenta con mayor frecuencia al público que desconoce del proceso del ataque y las alertas que debe tomar en consideración para no ser víctima de aquellos.

- Información relevante que puede comprometer son sistemas de pagos online, como datos de cuentas bancarias, números de documentos de identificación, entre otra información privada, puede encontrarse en redes sociales, sistemas de mensajería o directamente en listados disponibles en la web, que puede ser accesible con el uso de técnicas OSINT que utilizan información libre y de fuentes abiertas. Las mismas técnicas se pueden utilizar también para mitigar un ciberataque o emplearlas como acciones de ciberdefensa y bloquear los ataques. Muchos usuarios desconocen el tipo de ataque al que se pueden enfrentar o pueden ser víctimas; con este estudio se pretende instruir en la identificación de este tipo de ataques y como protegerse.
- En el caso del uso redes sociales, sistemas interorganizacionales y facilidades de software libre a nivel empresarial, la problemática se da frecuentemente por la falta de cuidado y desconocimiento del riesgo al que pueden estar expuestas las medianas y pequeñas empresas, que toman estas opciones ya sea por actualización tecnológica o por presión en el mercado.

Justificación

Los problemas de seguridad ligados a la gran accesibilidad de información en la web, la falta de cultura en el uso adecuado de la misma y el desconocimiento de las técnicas utilizadas por OSINT, hacen vulnerables los sistemas más avanzados de protección de datos, porque se refieren a las fallas humanas que pueden ser aprovechadas por técnicas de ingeniería social. La

escasez de información acerca de este tipo de ataques y del uso de técnicas de ciberdefensa relacionados, permiten una actividad importante de las amenazas sobre las vulnerabilidades especialmente humanas en el uso de sistemas informáticos relacionados con la web. Por esta razón es necesario realizar un análisis de OSINT, los ataques relacionados y sus componentes fundamentales, para determinar métodos y técnicas que permitan dar seguridad al usuario. Para esto se plantea el análisis de los ciberataques en el ámbito de las redes sociales y de información de fuentes abiertas.

Objetivos

Objetivo general

Desarrollar una propuesta metodológica, basada en el análisis de riesgos de seguridad informática en OSINT, para minimizar el impacto de los ciberataques mediante métodos y técnicas de ciberseguridad y ciberdefensa aplicando la norma ISO-27000.

Objetivos específicos

- Analizar el uso de métodos y técnicas de OSINT, basado en la investigación del estado del arte relacionado.
- Determinar la situación actual del riesgo de seguridad informática relacionada al uso de OSINT, utilizando estándares internacionales como COBIT e ISO 27000.
- Diseñar una propuesta metodológica para emplear de manera ética los métodos y técnicas de OSINT, tanto en ciberseguridad como en ciberdefensa.

Alcance

El presente proyecto comprende la identificación y comprensión de los métodos y técnicas de OSINT, para conocer su capacidad de empleo en diversos procesos tanto empresariales como de carácter individual en la protección, búsqueda y validación de información relevante,

considerando la legislación vigente de protección de datos personales e institucionales. Se pretende concebir nuevas visiones de empleo de las técnicas de OSINT, con procedimientos que permitan la protección contra ataques como los de Ingeniería Social en los que sistemas automáticos han fallado, a pesar del uso de técnicas de Inteligencia Artificial como Machine Learnig y otras.

Se analizarán casos actuales y estudios relacionados a OSINT para luego utilizar la metodología de análisis de riesgos y determinar los más significativos. A éstos riesgos se pretende aplicar un plan de tratamiento que permita reducir, evitar o transferir el riesgo mediante el uso de técnicas de manera sencilla e innovadora con el fin de determinar qué proceso debe seguir el usuario para no ser víctimas de amenazas externas que utilicen OSINT como técnicas de ataque, así mismo para aprovechar las características de OSINT para emplearlas en ciberseguridad y ciberdefensa por parte de equipos de respuesta ante incidentes informáticos.

Para delimitar de manera adecuada el alcance del proyecto, en la tabla Nro. 01 se proponen las preguntas de investigación relacionadas a los objetivos específicos.

Tabla 1:

Preguntas de investigación

Objetivo específico	Pregunta de investigación

i.	**Analizar el uso de métodos y técnicas de OSINT, basado en la investigación del estado del arte relacionado.**	• ¿Existen de métodos y técnicas específicas de OSINT, que se encuentran actualmente en uso efectivo?
ii.	**Determinar la situación actual del riesgo de seguridad informática relacionada al uso de OSINT, utilizando estándares internacionales como COBIT e ISO 27000.**	• ¿Es posible realizar un análisis del riesgo de seguridad informática relacionada al uso de OSINT, utilizando estándares internacionales como COBIT e ISO 27000?
iii.	**Diseñar una propuesta metodológica para emplear de manera ética los métodos y técnicas de OSINT, tanto en ciberseguridad como en ciberdefensa.**	• ¿Cómo se podría diseñar una propuesta metodológica para emplear de manera ética los métodos y técnicas de OSINT, tanto en ciberseguridad como en ciberdefensa?

Nota: Preguntas basadas en el análisis del proyecto.

El desarrollo de la propuesta metodológica permitirá mostrar información general de las técnicas utilizados para la detección de ataques en los que se utilice OSINT y también definir los procesos que se deben llevar a cabo para mitigarlos y proteger los datos de los usuarios mediante OSINT.

Capítulo II

Marco teórico

OSINT

Definición de OSINT

El término OSINT hace referencia a Open Source Intelligence, que se traduce como Inteligencia en Fuentes Abiertas, para la obtención y procesamiento de información obtenida de forma legal y ética de diferentes fuentes abiertas o públicas. Existen múltiples disciplinas de recolección de inteligencia como:

- SIGINT (Signals Intelligence): Inteligencia a partir de la intercepción de señales.
- GEOINT (Geospatial Intelligence): Inteligencia obtenida por medio de la geolocalización.
- HUMINT (Human Intelligence): Inteligencia adquirida por individuos, que interactúan con otras personas por medio de redes sociales y otros canales de comunicación.

Otras como ELINT (Electronic Intelligence), FININT (Financial Intelligence), IMINT (Imagery Intelligence), COMINT (Communication intelligence). El concepto de OSINT, bajo un nombre u otro, se ha desarrollado durante cientos de años. Con la llegada de las nuevas tecnologías de la información y comunicación se han centrado en Internet las posibles fuentes de recopilación de información, mediante la extracción de datos que puede ser realizada a partir de cualquier material público disponible como:

- Medios de comunicación: periódicos, revistas, radio y televisión de cualquier región del mundo.
- Internet: publicaciones online, blogs, grupos de discusión, medios ciudadanos (videos u otros contenidos creados por los usuarios), Youtube y otras redes sociales (Facebook, Twitter, Instagram, etc.).

- Datos públicos del gobierno (Boletines Oficiales del Estado): informes gubernamentales, presupuestos, audiencias, directorios de teléfono, conferencias de prensa, sitios web o discursos. A pesar de que estas fuentes provengan de fuentes oficiales, son de acceso público y pueden ser usadas abiertamente y gratuitamente.
- Publicaciones académicas y profesionales: información adquirida de revistas de artículos, simposios, conferencias, tesis, etc.
- Datos comerciales: imágenes, evaluaciones financieras e industriales y bases de datos.
- Literatura gris: informes técnicos, pre impresiones, patentes, documentos de trabajo, documentos comerciales, trabajos no publicados y boletines informativos.

Lo más importante a tener en cuenta es que OSINT no consiste en un trabajo de investigación en el que obtenemos diversos fragmentos de información acerca de un objetivo, si no que consiste en un proceso de inteligencia para crear un conocimiento personalizado para ese objetivo, que puede ser un individuo o grupo específico (Akaichi, 2014).

Características

En base de la historia de estos procesos, se puede establecer una serie de características de OSINT, que permiten definir sus puntos fuertes y sus puntos débiles, para elaborar análisis posteriores.

- Eficiente.- Desde el punto de vista de la inversión de recursos y el equilibrio que mantienen con el tiempo y los beneficios generados, OSINT es la forma de inteligencia que permite obtener más con menos y en el menor plazo.
- Rápido.- Antes de internet y luego de su aparición, el acceso a la información abierta permite efectuar de la forma más ágil el ciclo de inteligencia.

- Intermediado.- Cuando se utiliza OSINT se pesca en el mar de datos e información que otros han generado, de tal forma que las fuentes normalmente han pasado por al menos un intermediario, cuando no varios.
- Dependiente.- La existencia de intermediarios también indica la presencia de dos extremos, una fuente y un receptor, que respectivamente generan y sufren una dependencia, así mismo tienden a existir numerosos intermediarios en la forma de editores, periodistas, usuarios, medios, etcétera.
- Accesible.- El reducido coste económico de los medios que permiten a los individuos llenar el mar de información, es el mismo coste reducido que permite a los buscadores de información hacer OSINT, así pues cualquier individuo u organización pequeña o grande, rica o pobre, puede hacer uso de esta forma de inteligencia con un mayor o menor grado de éxito. Pero como siempre ha ocurrido, lo accesible y lo público, y lo secreto y lo sensible tienden a repelerse, por tanto, no es de esperar que lo más comprometido y sensible pueda ser siempre averiguado de la forma más óptima mediante OSINT.
- Voluminoso.- El mar de información siempre ha sido grande, pero con la llegada de la red global en la que cualquier individuo es una fuente de información, el volumen total se ha disparado hasta convertir a la fase de procesamiento (no a la de obtención), en el mayor reto.

Las características mencionadas permiten determinar cuáles son los pilares más débiles de OSINT y por tanto los más susceptibles de convertirse en fuentes de engaños o errores. Está claro que se puede utilizar OSINT, en poco tiempo, con pocos recursos y con un voluminoso acceso a distintas fuentes. Hay que considerar que no todas las materias están bien cubiertas por fuentes abiertas, por el contrario, existe una fuerte relación de dependencia entre el adquirente de la información, el suministrador y los medios o personas intermediarias.

Lo que a su vez se origina por el fácil acceso, que da lugar a la aparición de una gran cantidad de fuentes abiertas. Por tanto, un concepto clave es el V-OSINT u OSINT verificado, ya que la cantidad de fuentes no es proporcional a la posibilidad de comprobar su veracidad y en realidad, cualquiera puede verter información viciada, de ahí la necesidad de seguir un buen proceso de verificación de las fuentes fiables y de la aplicación del pensamiento crítico en el análisis.

Componentes

- Fuentes Abiertas

Las fuentes de información que se utilizan en un proceso OSINT pueden ser de diferente tipo. Dependiendo de los objetivos que se desean obtener, se han desarrolladas diversas herramientas para su explotación. A pesar de que se pueden realizar varias clasificaciones de las herramientas que extraen información de fuentes diferentes, una de ellas sería:

- Motores de búsqueda:

Una de las principales herramientas son los motores de búsqueda como Google, Bing, Yahoo o DuckDuckGo, se podría incluir una gran cantidad de metabuscadores o buscadores personalizados. Una de las principales características de estos motores es la capacidad para realizar búsquedas parametrizadas a través de los denominados dorks, lo que se conoce como Google o Bing Hacking.

Los motores de búsqueda surgieron a principios de los 90 debido a la necesidad de organizar, clasificar y gestionar la información de Internet, ya que cada vez surgían muchos sitios web llenos de contenido. Estos motores realizan una exploración permanente de Internet, indexando toda la información que encuentran, es decir, crean índices propios de todo el contenido que son capaces de rastrear.

Cada vez que estamos realizando una búsqueda en sitios como Google o Yahoo, estos consultan en su índice con el fin de entregar el resultado que consideran mejor.

El motivo de la indexación tiene que ver con la capacidad de reacción. El hecho de disponer de índice propio permite a los motores de búsqueda dar una respuesta rápida al usuario. El simple hecho de realizar búsquedas en Google, Yahoo, Bing o DuckDuckGo, permite el uso de una de las herramientas más útiles de extraer información en Internet. Sin embargo, muchos de estos navegadores ofrecen una serie de operadores avanzados que permiten realizar búsquedas parametrizadas para acceder a aquella información que es más difícil de localizar.

- Redes sociales:

Una de las fuentes más importantes para encontrar información sobre un objetivo son las redes sociales. El número de usuarios en las redes sociales crece y crece cada día más y muchos de nosotros solemos publicar muchos datos sobre nosotros mismos o nuestras vidas, los cuales poseen una veracidad extra al ser mostrados por nosotros mismos. Existen varias herramientas que nos permiten detectar la presencia de cualquier persona en estas redes sociales y muchas de estas tienen APIs de uso libre que pueden ser utilizados para la creación de buscadores avanzados.

- Datos de carácter personal:

Este tipo de datos que podemos encontrar en la red incluyen información muy concreta y precisa sobre nosotros mismos, tales como nombre, edad, lugar de residencia, lugar de trabajo, teléfono, etc. Existen varios buscadores especializados que con solo uno de estos datos pueden obtener toda la información que existe en Internet sobre nuestra persona.

- Datos corporativos:

También podemos encontrar datos generales sobre las empresas como teléfonos, correos, información sobre empleados u otros datos más avanzados como puede ser la propia infraestructura de red y sistemas a través de aplicaciones como Maltego.

- Casos de estudio efectos de Ciberataques

En las últimas décadas, en América Latina, pocos países van adhiriéndose a esta nueva iniciativa de vital importancia, porque la innovación disruptiva, las estrategias de protección digital, la protección contra posibles riesgos, los ataques cibernéticos, las tecnologías inteligentes, el IoT4y la adopción de la industria 4.0;obligan a desarrollar programas específicos de respuestas a estos posibles incidentes de ICS(Ciberseguridad en Infraestructuras Críticas), en donde las empresas, la sociedad, el gobierno y la defensa nacional dependen del buen manejo de las tecnologías de la información y la comunicación(TIC´s) y de la operación de las Infraestructuras Críticas de Información (ICIs), en donde todos los sectores públicos y privados se apoyan en la disponibilidad, integridad y confidencialidad dela información.

El auge de las TIC´s, la protección y la disponibilidad de los activos de información críticos, constituyen escenarios vulnerables a las amenazas que podrían afectar de manera crítica el buen funcionamiento de los sistemas informáticos, la banca, la industria, gobiernos y la economía

Caso 1:

Estonia,2007 En abril de 2007, las instituciones de Estonia se paralizaron por los ciberataques que sufrieron numerosas instituciones públicas, entre ellas, el Parlamento y varios ministerios, además de bancos, partidos políticos y medios de comunicación.

Numerosos botnets enviaron mensajes spam para colapsar los servidores, como consecuencia no servían los cajeros automáticos ni la banca online. Estonia tuvo que cortar toda la línea de Internet y formatear sus sistemas. Todo esto sucedió luego de que el gobierno estonio reubicara la estatua del soldado de Bronce de Tallin.

Caso 2:

EquifaxData Breach La empresa Equifax, en julio del 2017, sufrió el robo de nombres, números de seguro social, fechas de nacimiento, direcciones y, en algunos casos, números de licencia de conducir de residentes en EEUU, así como de personas en Reino Unido y Canadá. También administra datos sobre préstamos, pagos, tarjetas de crédito, límites de crédito, rentas y pagos de servicios públicos, entre otras informaciones.

Según informa Equifax, manejan los datos de más de 820 millones de personas y más de 91 millones de empresas en todo el mundo.

Caso 3:

Un informe presentado por el Instituto Nacional de Estadísticas y Censos (INEC 2016), en los últimos 5 años, el servicio de internet ha registrado un incremento del 22,5%en el 2012 y que llegó al 32,8% en el 2015. Esto hizo que el sector bancario incremente las ofertas de servicios en línea ej.: banca electrónica, transacciones electrónicas, etc.), así como otras entidades públicas, como el pago de los predios urbanos, pago de impuestos, matriculación y revisión vehicular, compras en línea en establecimientos de Ecuador, etc.

Estos avances tecnológicos hicieron surgir nuevos tipos de ataques hacia dispositivos móviles, como el primer caso del malware conocido como “Octubre Rojo”, que apareció en el 2007, y que robaba datos de teléfonos móviles, como smartphones (iPhone, Nokia y Windows Mobile).

Los ciberataques también tuvieron como objetivo el área de procesos electorales, donde se recomendó que los funcionarios tengan una formación en ciberseguridad para la toma de decisiones con precisión, porque los atacantes buscan y detectan debilidades en diferentes actividades ya sea en los sectores académicos, de comunicación, servicios, etc.

Caso 4:

En Ecuador, por decreto ejecutivo, se creó el Plan Nacional de Seguridad Integral (PNSI) 2014-2017, así como el Plan Estratégico Institucional 2015-2017, y dentro de las Fuerzas Armadas se creó el Comando de Ciberdefensa.

Así también fue creado elplandegobiernoelectrónico2014-2017, el cual incrementó los controles de calidad a las empresas que prestan servicios de internet, así como la creación de redes comunitarias en zonas rurales (Ministerio Coordinador de Seguridad, 2014), y las políticas de Gobierno para la transformación productiva y el desarrollo del Ecuador, entre otros.

Algunas Organizaciones Internacionales han promovido estrategias para afrontar las amenazas de ciberdefensa y ciberseguridad a diferentes países, como la publicación de varios documentos o estándares, entre ellos el National Cybersecurity Strategy Guide (ITU 2011)11La conformación del Grupo e-Justicia de Cumbre Judicial Iberoamericana y a la colaboración de cada uno de sus miembros, ponen a disposición el “Compendio Normativo sobre Ciberdelincuencia” como un aporte al Derecho, donde se podrá encontrar legislación sustantiva y procesal referente a los delitos informáticos.

Los aspectos relacionados con la estructura organizativa, jurisprudencial y convenios suscritos por sus respectivos países con información remitida por los Poderes Judiciales de: Chile, Colombia, Costa Rica, Ecuador, El Salvador, Guatemala, México, Nicaragua, Paraguay, Portugal, República Dominicana y Uruguay.

El análisis de este documento, se basa en las posibles formas de ciberataques y las medidas de protección, a tomarse en cuenta para minimizar o controlar cualquier riesgo. En el 2014, se registró un aumento de 37% de robos a la banca virtual, 14% en tarjetas de crédito y 46% en cajeros electrónicos (Ministerio Coordinador de Seguridad 2014). Pero estos inconvenientes no han sido solo en los sistemas de la banca, también los supuestos ataques cibernéticos procedentes de Colombia, Estados Unidos, Rusia, China y Francia sobre cuentas o datos personales de ciudadanos ecuatorianos, portal es web de opinión libre (ElUniverso2016), entre otros. Como se puede apreciar en la siguiente imagen, la revista Forbes (2018), muestra seis posibles formas de ciberataques (Bernard et al., 2018).

Descripción de las técnicas de OSINT

- Proceso

Se trata de un proceso que consiste en generar inteligencia (entendiendo inteligencia como el análisis y procesamiento de los datos para que puedan ser correctamente utilizados) a partir de la información extraída de distintas fuentes públicas en Internet o en otros medios tradicional espera la investigación de un objetivo. Cuando hablamos de estas fuentes abiertas, nos referimos a aquellos puntos clave dentro de Internet donde podemos encontrar información acerca de personas, lugares o instituciones de forma pública, por lo que su acceso y recolección se encuentra dentro del marco legal.

Entre las distintas fuentes disponibles, destacan los motores de búsqueda, ya que son los encargados de indexar gran parte de la información disponible en la red; las redes sociales, que debido al exceso de confianza de la gente a la hora de publicar aspectos de su vida privada se han convertido en uno de los principales puntos de acceso a datos críticos sobre los posibles objetivos.

Los distintos datos tanto de carácter personal como corporativo que podemos obtener a través de diferentes medios, y a partir de los cuales podemos realizar diferentes tipos de búsqueda para obtener aún más información.

Los distintos gobiernos que basan sus procesos de inteligencia en su habilidad para adquirir todo tipo de datos tienen su propio uso de OSINT. Sin embargo, al final del día, todos usamos OSINT: cuando realizamos búsquedas en Internet para comparar distintos tipos de productos que queremos comprar o para encontrar alguna persona a la que queremos conocer, estamos básicamente adquiriendo y seleccionando datos de fuentes abiertas. Tal es la importancia de la inteligencia en fuentes abiertas, que cada vez más organizaciones están desarrollando sus propias estrategias de OSINT.

Las correctas herramientas, combinadas con las habilidades de equipos de profesionales dedicados a la búsqueda de información, pueden ayudar a estas organizaciones de forma cada vez más efectiva, proporcionando apoyo en la disminución de riesgos gracias al conocimiento estadístico y predictivo del análisis de grandes volúmenes de información. Todo esto hace que OSINT cobre cada vez más importancia dentro del ámbito de la ciberinteligencia. La ciberinteligencia permite, a partir de la adquisición y análisis de la información, identificar, rastrear, predecir y contrarrestar las capacidades, intenciones y actividades de los atacantes, y ofrecer cursos de acción con base en el contexto particular de la organización, que mejoren la toma de decisiones. A parte de proveer de dicho apoyo a las organizaciones, permiten mantener la seguridad de todos los ciudadanos gracias a su uso en varios frentes como la lucha contra el terrorismo o la persecución de distintos tipos de delincuentes informáticos (Senekal & Kotzé, 2019).

Para resumir, algunos de los ejemplos de la utilización de OSINT pueden ser los siguientes:

- Conocer la reputación online de un usuario o empresa.

- Realizar estudios sociológicos, psicológicos, lingüísticos, etc.
- Auditorías de empresas y otros tipos de organismos con el fin de evaluar el nivel de privacidad y seguridad.
- Evaluación de las distintas tendencias de los mercados.
- Identificación y prevención de posibles amenazas en el ámbito militar o la seguridad nacional.
- Por otro lado, también puede tener usos negativos, ya que puede ser utilizado por ciberdelincuentes para lanzar distintos tipos de ataques contra organizaciones o personas.

- Fases de la inteligencia

Como hemos comentado anteriormente, la extracción de datos en fuentes abiertas forma parte de un proceso aún mayor que utiliza estos datos extraídos para generar inteligencia. Para empezar, tenemos que tener en cuenta los problemas que pueden surgir en el desarrollo de este proceso. Algunos de estos problemas pueden ser:

- Demasiada información: como ya se ha puesto de manifiesto, la cantidad de información pública disponible en Internet es más que notable. Es por ello, que se debe realizar un proceso exhaustivo para identificar y seleccionar las fuentes de información más importantes que van a ser recopiladas y que servirán en la generación de inteligencia.
- Fiabilidad de las fuentes: es importante valorar previamente las fuentes de las que se va a realizar la recopilación, ya que una selección errónea de las mismas puede provocar desinformación o resultados equivocados. Por todo esto, se recomiendan una serie de fases o pasos a seguir para el desarrollo de este proceso y que se basa en el denominado ciclo de inteligencia. Las fases de este ciclo son las siguientes:

Figura 1

Técnicas de OSINT

Nota: Gráfico donde representa las técnicas en ciclo de OSINT. (Akaichi, 2016)

- Requisitos: Establecer los requerimientos que se quieren cumplir. Los objetivos que se desean obtener, la información que se quiere tener y el tiempo que se va a necesitar.
- Fuentes de información: Encontrar las fuentes de información más relevantes que serán utilizadas para obtener la información. Además, se deberá realizar una planificación, definiendo cuál será la estrategia para la recolección de información, el tipo de información y el contenido, definiendo y clasificando la disponibilidad y fiabilidad de las fuentes y los flujos de la comunicación.
- Adquisición: Consiste en conseguir la información de las diversas fuentes de información públicas que se han identificado en la fase anterior, es decir, obtener la información en bruto.

Cuanta mayor cantidad de información consigamos mejor, pero siempre debemos tener en cuenta los distintos atributos relacionados con esta información como su contexto, fiabilidad de las fuentes, integridad, fecha, etc. Estos atributos serán importantes en el desarrollo de las siguientes fases. Además, la extracción de datos debe realizarse bajo un marco legal, ya que de lo contrario se podría anular la eficacia de los resultados. Para ello, nos serviremos de las distintas herramientas disponibles y que veremos más adelante en este trabajo.

- Procesamiento: En esta fase se procesará la información conseguida para proveerla de un formato de manera que posteriormente pueda ser analizada.
- Análisis: Se genera inteligencia a partir de los datos recopilados y procesados. En esta fase se analizará la información obtenida, y que, tras depurarla, tratarla y procesarla, se eliminará aquella que sea inservible debido a que carezca del suficiente valor, sea errónea, o no sea lo suficientemente veraz para incluirla. Para ello, se necesita de un equipo de personas que clasifiquen la información en función de los atributos asociados a la fiabilidad de la fuente, fiabilidad de la información, validez de los datos, pertinencia, relevancia y utilidad.
- Inteligencia: Presentar la información conseguida de una manera eficaz, potencialmente útil y comprensible, gracias a informes detallados con diagramas, tablas o figuras para que se puedan sacar las conclusiones pertinentes sobre dicha información (Akaichi, 2016).

Riesgos

Definición

La palabra riesgo es tan antigua como la propia existencia humana. Podemos decir que con ella se describe, desde el sentido común, la posibilidad de perder algo (o alguien) o de tener un resultado no deseado, negativo o peligroso.

El riesgo de una actividad puede tener dos componentes: la posibilidad o probabilidad de que un resultado negativo ocurra y el tamaño de ese resultado. Por lo tanto, mientras mayor sea la probabilidad y la pérdida potencial, mayor será el riesgo.

Cada vez que tomamos una decisión y valoramos la relación costos-beneficios, no estamos sino evaluando los riesgos que corremos con esa decisión y las ventajas o desventajas que esta nos puede traer. Es decir, funcionamos cotidianamente con la noción de riesgos aunque no seamos conscientes de ello en todo momento. Por lo tanto, ni la palabra riesgo ni el fenómeno que se describe con ella son nuevos para nuestro entendimiento, al contrario, el ser humano desde sus inicios como especie convivía naturalmente con los riesgos y reaccionaba intuitivamente ante ellos.

Solo a partir de determinado momento en el desarrollo de las sociedades humanas el riesgo se convirtió en una preocupación consciente de las personas. Mucho después, con el desarrollo tecnológico y científico, esta definición fue introduciéndose en el terreno de la ciencia y se convirtió actualmente en un "concepto dinámico y multifacético con ramificaciones científicas, económicas, sociales y políticas", lo cual quiere decir que profesionales de las más diversas ramas del saber han hecho suyo el estudio de las distintas facetas del riesgo más allá de las consideraciones cotidianas (Akaichi, 2014).

Actualmente la preocupación de la sociedad por el riesgo está muy relacionada con la complejidad que se vive. La aceleración de los cambios sociales, económicos y políticos, la globalización y la progresiva industrialización traen aparejadas la contaminación ambiental, la escasez de recursos naturales vitales como el agua, accidentes industriales que han socavado la seguridad pública, la proliferación de determinadas enfermedades (tanto en humanos como en animales y plantas), transformaciones irreversibles del medioambiente, entre otras.

El ritmo actual de cambios reduce la estabilidad social e institucional a largo plazo afecta la facultad de predecir el futuro y, por tanto, aumenta la incertidumbre. Ha aumentado también la conciencia sobre el riesgo, y en consecuencia, la intolerancia donde también las personas se esfuerzan por protegerse de las catástrofes y del efecto de esos riesgos ilocalizables, indefinidos y con dimensiones no previstas.

Por otra parte, al mismo ritmo que crece la industrialización, fomentada básicamente por el primer mundo desarrollado y la preocupación por sus consecuencias para nuestro planeta, también se incrementa la preocupación internacional por la proliferación de las enfermedades infecciosas y no transmisibles, en cuyo tratamiento se consumen grandes recursos. El enfoque hacia este tipo de enfermedades ha ido incrementando las acciones preventivas tanto para la preservación misma de la vida y la disminución de las tasas de morbilidad por estas enfermedades, como para la reducción de los costos en salud pública por concepto de tratamientos médicos.

El riesgo a enfermar aparece entonces como otra de las grandes preocupaciones en la sociedad actual, aunque las estrategias de enfrentamiento al mismo varían de acuerdo con el contexto socioeconómico y político, las condiciones de vida y el cuadro epidemiológico que caracterice a cada zona o región.

Todo lo anterior explica por qué los más disímiles profesionales se interesan por la problemática del riesgo, desde economistas, inversionistas, especialistas en seguros de todo tipo, publicistas, salubristas, pedagogos, psicólogos, ingenieros, ambientalistas, hasta militares, ministros, presidentes y funcionarios de organismos internacionales. Es por eso que los estudios sobre riesgo no son patrimonio exclusivo de ningún campo de investigación o esfera de la vida social, aunque en cada una de ellas la investigación o aplicación de esta definición alcanza matices particulares.

En ese sentido los estudios de percepción del riesgo han sido muy importantes en el encauzamiento de las acciones preventivas ante epidemias sociales como lo constituyen el SIDA, el alcoholismo y la accidentalidad, pero también en el enfrentamiento de catástrofes naturales, accidentes nucleares y en la protección de especies animales en vías de extinción, por sólo citar algunas de las más importantes preocupaciones de la población en el mundo contemporáneo. Exploremos entonces algunos aspectos que no deben dejarse de tomar en cuenta cuando se intenta comprender los significados del concepto "riesgo".

- Aspectos relevantes en las definiciones del riesgo

Uno de los retos que actualmente presenta la investigación del fenómeno del riesgo es la variedad de aspectos que se incluyen en su definición y la manera particular en que los científicos los interpretan. Por ejemplo, el Diccionario de la Lengua Española, en su edición electrónica del año 1995, remite la palabra riesgo al antiguo vocablo rasgar, cortar, que a su vez se origina en el latín resecare, cortar. En esta versión se define al riesgo de dos formas:

- Contingencia o proximidad de un daño

En este caso se destaca más que todo el sentido futuro del término, algo que puede acontecer. Otras definiciones del riesgo se refieren a la probabilidad de ocurrencia de un evento dado. El concepto también se asocia a variedad de medidas de probabilidad de un resultado generalmente no favorable, al número esperado de pérdidas humanas, personas heridas, propiedad dañada e interrupción de actividades económicas, producto de fenómenos naturales particulares y, por consiguiente, de riesgos específicos y elementos de riesgo.

- Posibilidad de pérdidas, de lesiones, de desventajas o de destrucción:

Alguien o algo que produce o sugiere una situación riesgosa o una posibilidad adversa: un elemento o factor peligroso más frecuentemente citado con calificativos para indicar el grado o tipo de peligro.

- Posibilidad de pérdida o de peligro para el objeto o el asegurado cubierto por el contrato:
    - El grado de posibilidad de dicha pérdida.
    - Monto en riesgo.
    - Persona o cosa que a juicio del asegurador resulta peligrosa.
    - Una situación riesgosa para lo asegurado proveniente de una causa o de una fuente especificada.
    - El producto del monto que podría perderse por la probabilidad de perderlo, comparado con la expectativa.

Este conjunto de definiciones abarca varias aristas del riesgo. Se considera como tal la posibilidad y la probabilidad de una pérdida en su más amplio sentido; la persona, cosa o situación que puede producir ese efecto; el monto de la pérdida por riesgo así como el valor o monto mismo del riesgo.

Esta amplitud de definiciones unida a la diversa comprensión de este término en las diferentes culturas e idiomas, permiten darnos cuenta del complejo panorama que se presenta en el ámbito científico internacional alrededor de este término (Gómez et al., 2010a).

Metodología de análisis de riesgos

- Introducción

Con el crecimiento y auge de las Nuevas Tecnologías de la Información y la Comunicación (NTIC), los avances en los servicios y modelos de comunicaciones e información, el uso continuo y generalizado a nivel global de la Internet; también se han aumentado los ataques a los sistemas informáticos, lo que ha llevado a las empresas a buscar estrategias que les permitan ejecutar análisis que prevengan, controlen y reduzcan los riesgos asociados a la violación o vulnerabilidad de su información. El alcance de los objetivos propuestos, los eventos que pueden desencadenar un incidente que produzca daños en sus activos, la posibilidad de la materialización de una amenaza, las consecuencias de la misma, la posibilidad de que se genere un impacto en los bienes de la organización y finalmente los procedimientos que se llevan a cabo para reducir un riesgo.

“El análisis de riesgos pretende dar respuesta a tres interrogantes: saber qué se quiere proteger, contra quién y cómo se va a hacer”. Es de vital importancia que en las empresas se establezcan objetivos empresariales a partir de ellos, políticas de seguridad que permitan controlar la realización de los procesos para así optimizar el análisis de riesgos. El imperativo estudio en las empresas, se debería garantizar la continuidad del negocio, asegurando los principios de la seguridad de la información.

Las organizaciones están expuestas día a día a amenazas tanto internas como externas que ocasionan robo de identidad e información, bases de datos, información sensible de clientes, pérdida de credibilidad y daños financieros que pueden afectar la sostenibilidad de la entidad.

Por lo anterior, se cuestiona si las empresas conocen y aplican metodologías para el análisis de riesgos y protección de los principios de seguridad de la información o por el contrario desconocen los modelos que traigan protección de los principios de seguridad de la información.

Mediante esta investigación se darán a conocer las diferentes metodologías soportadas, utilizando para ello un caso de estudio aplicado a una organización, las razones por las que es importante su aplicación y finalmente recomendaciones sobre el modelo que se considera brinda una mejor oportunidad de toma de decisiones ante un riesgo inminente.

Existen metodologías que permiten hacer un uso adecuado del análisis de riesgos y así asegurar los sistemas de información de las organizaciones.

- OCTAVE

La metodología OCTAVE (Operationally Critical Threats Assets and Vulnerability Evaluation), desarrollada por el Equipo de Respuesta ante Emergencias Informáticas (CERT, por sus siglas en inglés), evalúa los riesgos de seguridad de la información y propone un plan de mitigación de los mismos dentro de una empresa. Por tanto, se tienen en cuenta las necesidades de la empresa donde se está implementando, permitiendo reducir los riesgos de seguridad de información, para lograr una mayor protección a estos elementos dentro del sistema. OCTAVE equilibra aspectos de riesgos operativos, prácticas de seguridad y tecnología para que a partir de éstos, los entes empresariales puedan tomar decisiones de protección de información basado en los principios de la seguridad de la información. Esta metodología persigue dos objetivos específicos que son: concientizar a la organización que la seguridad informática no es un asunto solamente técnico y presentar los estándares internacionales que guían la implementación de seguridad de aquellos aspectos no técnicos.

Hasta la fecha han sido publicadas varias metodologías de este tipo: OCTAVE que ha sido definida para grandes organizaciones de trecientos o más empleados, OCTAVE – S que se enfoca para pequeñas empresas, por ejemplo, PYMES con veinte a ochenta empleados y finalmente, OCTAVE ALLEGRO que permite analizar riesgos con mayor enfoque en activos de información, cada una de estas metodologías ejecuta las fases mencionadas con algunas variaciones dependiendo de las necesidades.

Con una metodología de análisis de riesgos como OCTAVE la empresa puede obtener beneficios como: dirigir y gestionar adecuadamente sus evaluaciones de riesgos, tomar decisiones basándose en los mismos, proteger los activos de información y, por último, comunicar de forma efectiva la información clave de seguridad los cuales se derivan de las siguientes características: en primera medida, se establecen equipos auto dirigidos dentro de la organización con la finalidad de dar solución a las necesidades de seguridad que esta puede tener.

Y por otro lado, se dice que este método es FLEXIBLE ya que es adaptable a todo tipo de organización independientemente del entorno porque se basa en los riesgos, la capacidad de recuperación y la experiencia que se tenga en este tema.

Finalmente, es importante mencionar que OCTAVE busca asegurar la continuidad del negocio, identificar y medir riesgos, establecer controles para mitigarlos, conservar la información (activo importante) e intervenir en todas las dependencias de la organización, ya que de esta manera puede aprovechar al máximo el conocimiento de los distintos niveles de la empresa (Gómez et al., 2010b)

- MEHARI

MEHARI (Method for Harmonized Analysis of Risk), es definida por la organización francesa especializada en la seguridad de los sistemas de información (CLUSIF) como una metodología que proporciona un conjunto de herramientas que permiten hacer un análisis.

Los cuales son de riesgos cualitativo y cuantitativo, cuando sea necesario para tener una adecuada gestión de seguridad. De lo anterior, se deduce que está diseñada para acompañar los procesos de análisis de riesgos empresariales tanto actuales como futuros. En la metodología MEHARI se hace un análisis de la seguridad basado en tres criterios básicos: confidencialidad, integridad y disponibilidad (Gómez et al., 2010b).

- MAGERIT

MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) es reconocida por ENISA (Agencia Europea de Seguridad de las Redes y de la Información) y promovida por el Consejo Superior de Administración Electrónica con el fin de sistematizar el análisis de los riesgos que pueden presentar los activos de una organización.

Esta metodología es importante porque el crecimiento de la tecnología dentro de las organizaciones se está dando de manera exponencial y, por lo tanto, es necesario minimizar los riesgos asociados al uso de los sistemas garantizando la autenticidad, confidencialidad, integridad, disponibilidad y trazabilidad de los mismos, con la finalidad de generar confianza en los clientes tanto internos como externos de la organización; de igual manera, presenta una guía de cómo llevar a cabo el análisis de riesgos y se divide en 3 libros, el primero describe la estructura del modelo de gestión de riesgos, el segundo presenta el inventario para enfocar el análisis de riesgos y el último compila una guía de técnicas de trabajo para dicho fin.

MAGERIT fue creada con el fin de cumplir con objetivos como conocer el estado de seguridad de los sistemas de información y la implementación de medidas de seguridad, garantizar que no hayan elementos que queden fuera del análisis para que haya una profundidad adecuada en el mismo, mitigar las vulnerabilidades y asegurar el desarrollo del sistema en todas las fases de desarrollo.

Estos objetivos han posicionado a MAGERIT como una de las metodologías más utilizadas en el ámbito empresarial ya que les permite prepararse para procesos de auditorías, certificaciones y acreditaciones (Gómez et al., 2010b).

- CRAMM

CRAMM (CCTA Risk Analysis and Management Method), es el método de análisis y control de riesgos de la Central Computer and Telecommunications Agency (CCTA) del gobierno británico, permite identificar, medir y reducir al mínimo los ataques a los que están expuestas las organizaciones día a día y es definida como una metodología que aplica los conceptos de manera formal, estructurada y disciplinada protegiendo los principios de seguridad de la información de un sistema y de sus activos.

Cabe resaltar que CRAMM realiza un análisis de riesgos cualitativo y cuantitativo por lo que se conoce como una metodología mixta, ésta se apoya de una herramienta de gestión, lo que permite a las organizaciones tener una visión clara y priorizada de las amenazas a las que está expuesta y que pueden afectar los recursos y la continuidad del negocio, basándose en una matriz donde las filas representan los activos y las columnas los riesgos que podrían afectar la integridad, disponibilidad y confidencialidad de los mismos, por otro lado, CRAMM proporciona información acerca de las características de funcionamiento del sistema y una identificación profunda y clara de los activos que se encuentran más expuestos.

Los elementos que se deben tener en cuenta para realizar un adecuado análisis de riesgos con la metodología CRAMM son: activos, vulnerabilidades, riesgos, amenazas, contramedidas, implementación y auditoría, los cuales permiten obtener un mejor resultado y asegurar la continuidad de negocio (Gómez et al., 2010b).

- EBIOS

EBIOS (Expresión de las Necesidades e Identificación de los Objetos de Seguridad), es una metodología francesa de gestión de riesgos, fue creada por la dirección Central de seguridad de los sistemas de Información de Francia DCSSI.

La comunicación con los clientes internos y externos para contribuir al proceso de la gestión de riesgos de seguridad de los sistemas de información, de igual manera, ayuda a la empresa a tener un mayor reconocimiento en sus actividades de seguridad ya que esta tiene compatibilidad con las normas internacionales como la ISO.

Este procedimiento permite a la organización tener un mayor conocimiento de sus activos y las necesidades de seguridad identificando las amenazas y vulnerabilidades a las que se encuentran expuestos para su posterior mitigación (Gómez, Pérez, Donoso, & Herrera, 2010).

- NIST SP 800:30

SP 800:30 (Guía de Gestión de Riesgos de los Sistemas de Tecnología de la Información), es un estándar desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST), fue formulado para la evaluación de riesgos de seguridad de la información especialmente a los sistemas de TI (Tecnología de la Información), proporciona un guía para la seguridad de las infraestructuras de la misma desde una perspectiva técnica. Por otro lado, esta guía provee fundamentos para la administración de riesgos así como la evaluación y mitigación de los riesgos identificados dentro del sistema de TI con el objetivo de apoyar a las organizaciones con todo lo relacionado a Tecnología.

La metodología NIST SP 800:30 está compuesta por nueve fases: caracterización del sistema, la cual permite establecer el alcance y los límites operacionales de la evaluación de riesgos en la empresa; identificación de amenazas, es donde se definen las fuentes de motivación de las mismas; identificación de vulnerabilidades.

En esta fase desarrolla una lista de defectos o debilidades del sistema que podrían ser explotadas por una amenaza; análisis de controles; determinación de la probabilidad; análisis de impacto; fase de determinación del riesgo, ayuda a evaluar el riesgo en el sistema de información, recomendaciones de control en donde se proporcionan los controles que podrían mitigar el riesgo identificado disminuyéndolo hasta un nivel aceptable, finalmente está la documentación de resultados la cual genera un informe con la descripción de amenazas y vulnerabilidades, midiendo el riesgo y generando recomendaciones para la implementación de controles.

- *Metodología a utilizar*

Mediante el estudio y análisis competente acerca de las metodologías para la mitigación del riesgo tomando en consideración el análisis de las técnicas OSINT la que mayor efectividad puede tener en el proceso es OCTAVE ya que cuenta con procesos de evaluación y análisis de acuerdo a las amenazas y vulnerabilidades.

Amenazas que afectan a los sistemas de información

Alertas de amenazas

La seguridad informática, de igual manera a como sucede con la seguridad aplicada a otros entornos, trata de minimizar los riesgos asociados al acceso y utilización de determinados sistemas de forma no autorizada y en general malintencionada.

El objetivo de la seguridad informática es proteger los recursos informáticos valiosos de la organización, tales como información, hardware o software. A través de la adopción de las medidas adecuadas, la seguridad informática ayuda a una organización a cumplir sus objetivos, permite proteger los recursos financieros, sistemas de información, reputación, situación legal, y otros bienes tanto tangibles e intangibles.

En efecto, gestionar la seguridad informática organizacional es una tarea exigente y evaluar el valor de las tecnologías de seguridad es esencial para gestionar eficazmente la seguridad de la información.

El modelo presenta el diagrama causal de una empresa sin medidas de seguridad, la cual actúa únicamente en caso de que un ataque se convierta en un incidente. Las variables consideradas en este escenario son: tasa información, vulnerabilidades, ataques, nuevos incidentes, e inversión como se muestra en la siguiente imagen:

Figura 2

Empresa sin seguridad informática

Nota: Ejemplo de proceso de una empresa de seguridad informática. (Amaya Balaguera, 2015).

Si se invierte en solventar el ataque, no se resuelve el problema porque se descuida otro donde sí se debería invertir, ya que no se tiene un plan definido y no se conocen las necesidades de seguridad, lo que aumenta la vulnerabilidad porque se invierte en algo que no requería mayor atención y se deja de hacer en otra que sí.

En la Figura 2, se presenta el ciclo de refuerzo R1, en donde se acentúa el problema de la vulnerabilidad.

PHISHING

Método de suplantación de identidad, y utilizado para obtener datos confidenciales sin autorización. Según reportes y estadísticas el malware es quien causa la mayor cantidad de incidentes de seguridad, así que por lo mismo es uno de los dolores de cabeza de todas las organizaciones y personas en general, ya que cada día está más y más en aumento, logrando que se materialicen los riesgos a los que se están expuestos.

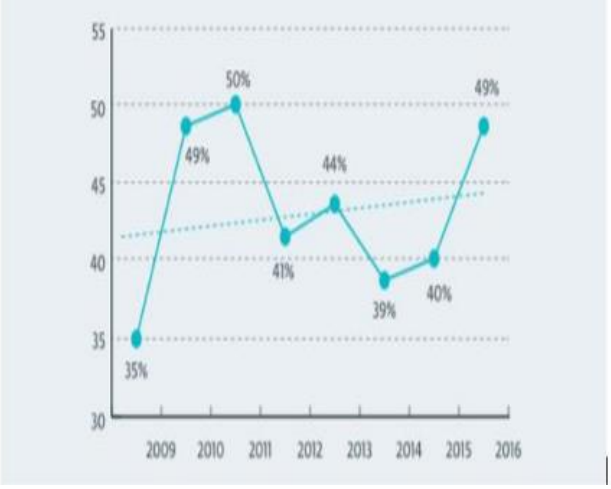
Muchos de estos se utilizan para extorsionar, cifrando toda la información que se tenga en el sistema y solicitando un rescate para lograr que el usuario logre acceder de nuevo a su información. El pago de algunos de estos rescates acrecienta a que por ejemplo este tipo de técnica utilizada y conocida como ransomware se vuelva más popular y mute cada vez más fuerte.

Esto es solo un ejemplo de los diferentes tipos de malware que se conocen, por lo que imaginen que tanto daño generan a todos ya sea con robo o pérdida de información personal, confidencial y también corporativa, que puede ser para espiar o adquirir datos clasificados y relevantes no solo de la empresa sino también de los clientes.

En el siguiente gráfico se puede evidenciar el constante avance del malware durante el año anterior en Latinoamérica, para ser más exactos se llegó a un 49% de infecciones por este tipo de software malicioso:

Figura 3

Mapa de infección con Malware.



Nota: Grafico del proceso que puede realizar el Malware en una empresa. (Amaya Balaguera, 2015)

En Colombia el índice fue también cerca al promedio general, ya que se registró un 46,7% de infecciones por este tipo de amenaza, convirtiéndolo en el tercer país más afectado de la región:

El phishing es una técnica, que mediante suplantación de correos electrónicos o páginas web, intenta obtener información confidencial de los usuarios, desde números de tarjetas de crédito hasta contraseñas.

Por otro lado los casos más populares de esta amenaza se tienen a los ciberdelincuentes que se hacen pasar por alguna persona conocido alguna entidad importante, desde la cual envían un mensaje de correo a la víctima objetivo, en el cuales le pide por medio de algún enlace falso a una supuesta página real, que ingrese datos como usuario y contraseña de acceso a alguna plataforma, teniendo como excusa verificar su cuenta o que presenta algún tipo de bloqueo y se necesita para restaurarlos, lo cual sucede con más frecuencia en el sector financiero, pero no se descarta en los demás.

Cuando la víctima digita sus datos en la supuesta página real, estos quedan almacenados en una base de datos del ciberdelincuente, el cual puede utilizar para fines de robo u otro tipo de información, donde se afectan la reputación y prestigio de dichas compañías.

Al igual producen distintos tipos de afectaciones a las personas del común que también caen frecuentemente en este tipo de estafa y que llega a tener un valor diferente a la información obtenida.

En la siguiente gráfica se pueden observar los resultados y el reporte del año anterior 2016 respecto a incidentes de phishing en la región, donde Colombia se vio afectada con 12,6%, si se compara con los demás países, se logra ver que ocupa el puesto 12, reflejando mejoría respecto a los demás, pero que no quiere decir que deba bajar la guardia frente a esta amenaza, antes esto ayuda a combatirla con más fuerza por medio de diferentes campañas privadas y de entidades del estado para lograr disminuir este engaño.

Figura 4

Incidencia de phishing en Latinoamérica.

Nota: Grafica de porcentajes de la influencia de phishing en Latinoamérica. (Amaya Balaguera, 2015)

Para contrarrestarlo existen algunas recomendaciones importantes, tanto a nivel hogar como corporativo:

- Pase el ratón por encima del enlace sospechoso (sin dar clic) para ver la url y saber si esta tiene algo que ver con la empresa que envía el email. Los criminales pueden intentar forzarte a entrar a una página falsa.
- Revise los correos electrónicos con relación apalabras mal escritas, saludos estándar y ausencia de contactos, dominios url incorrectos, imágenes poco profesionales y sospechosas con remitentes desconocidos. Estos puntos suelen ser habituales en phishing.
- Introduzca su nombre de usuario y contraseña solo cuando la conexión sea segura. Si ve el prefijo “https” antes de la url de la página, significa que todo está bien. Si no tiene la “s” (segura) –tenga cuidado.
- Nadie le va a pedir su contraseña. Su banco u otra entidad no le va a pedir su número de cuenta, ni su red social favorita le va a solicitar su contraseña de acceso.
- No haga clic en los links en cualquier correo electrónico enviado de remitentes desconocidos o sospechosos.
- No envíe correos electrónicos que parezcan sospechosos a demás colaboradores ya que esto podría extender el ataque a más personas.
- No responda correos no deseados que lleguen a su bandeja de entrada.
- No descargue contenido que su navegador o software de seguridad le alerte, puede ser malicioso.
- No entregue información personal como su usuario, contraseña de red, número de tarjeta de crédito, a un sitio o dirección de correo electrónico que piense puede ser sospechoso. Adicionalmente para un análisis más profundo de este ciberdelito.

- En las organizaciones se pueden seguir los siguientes pasos por personal capacitado, que pueda realizar unas validaciones respecto a los correos sospechosos que puedan recibir en algún momento de su día a día laboral, todo esto con el apoyo de algunas herramientas en línea gratuitas que son fácil de utilizar :
    - Análisis: Valide el tipo de correo que llega, el cual puede contener básicamente cualquier contenido que pueda parecer sospechoso, sin importar si viene de un remitente de confianza.
    - Luego de esto, trabaje sobre el correo sospechoso; y ábralo para revisar su contenido. En él es importante que se revise el remitente, cuáles son las cuentas destino, que tipo de asunto trae, contenido de archivos adjuntos, y si en el cuerpo del mensaje hay enlaces a otras páginas que puedan resultar sospechosas.
    - Revise de que trata su contenido, e identifique los posibles enlaces a sitios no deseados, o si contiene archivos adjuntos que puedan ser peligrosos.

Ingeniería social

La ingeniería social, se conoce como la ciencia y arte de hackearon más acorde al vocablo popular al arte del engaño seres humanos, el cual ha venido aumentado su popularidad durante estos últimos años. Gracias en parte a los avances tecnológicos y las comunicaciones, ya que cada día la población está más conectada entre sí con todo el mundo.

Vulnerabilidades de los sistemas de información

Ataques basados en vulnerabilidades

El proyecto abierto de seguridad en aplicaciones web (OWASP por sus siglas en inglés) emite el top 10 de las vulnerabilidades más graves de aplicaciones web (Lai, Grad. Inst. of Inf. & Comput. Educ., Wu, Chen, & Wu, 2008).

El objetivo principal es educar a las organizaciones que hacen uso de las TICs sobre las consecuencias de las vulnerabilidades de seguridad en aplicaciones web más importantes (Bernard et al., 2018). Los principales 5 ataques son:

- Inyección: Las fallas de inyección, tales como SQL, OS, LDAP, ocurren cuando datos no confidenciales son enviados a un intérprete como parte de un comando o consulta, tratando de engañar al intérprete en ejecutar comandos no intencionados o acceder datos no autorizados.
    - Secuencia de Comandos en Sitios Cruzados: Las fallas XSS ocurren cada vez que una aplicación toma datos no confidenciales y los envía al navegador web sin una validación y codificación apropiada. XSS permite a los atacantes ejecutar secuencia de comandos en el navegador de la víctima los cuales pueden secuestrar las sesiones de usuario, destruir sitios web, o dirigir al usuario hacia un sitio malicioso.
    - Configuración de Seguridad Incorrecta: Una buena seguridad requiere tener definidas e implementada una configuración segura para la aplicación, marcos de trabajo, servidores de aplicación, servidores web, base de datos, y plataformas. Todas estas configuraciones deben ser definidas, implementadas, y mantenidas ya que por lo general no son seguras por defecto.
- Exposición de datos sensibles: Muchas aplicaciones web no protegen adecuadamente datos sensibles tales como números de tarjetas de crédito, o credenciales de autenticación. Los datos sensibles requieren de métodos de protección adicionales tales como el cifrado de datos, así como también de precauciones especiales en un intercambio de datos con el navegador.

- Falsificación de Petición en Sitios Cruzados (CSRF): Un ataque CSRF obliga al navegador de una víctima autenticada a enviar una petición HTTP falsificado, incluyendo la sesión del usuario y cualquier otra información de autenticación incluida automáticamente, a una aplicación web vulnerable.
- Técnicas para detección de vulnerabilidad.

De acuerdo a los resultados obtenidos de la revisión sistemática sobre las herramientas y técnicas más utilizadas actualmente para detección de vulnerabilidades, se pueden establecer las siguientes:

- Black-box: Es una técnica basada para descubrir vulnerabilidades en aplicaciones web, probando la aplicación desde el punto de vista del atacante (Sreenivasa & Kuman, 2012).
- White-box: Está del lado del servidor. En este tipo de enfoque se tiene acceso a información relevante de la organización (Sreenivasa & Kuman, 2012).
- Análisis estático de código (auditoria de código fuente): Es un método en el que no se requiere ejecutar el programa, este realiza un análisis de código fuente directo para determinar huecos en la seguridad (Sreenivasa & Kuman, 2012).
- Análisis dinámico de código: Se comunica con la aplicación web a través de front-end de la aplicación en orden de identificar vulnerabilidades de seguridad potenciales y debilidades en la arquitectura de la aplicación web (Sreenivasa & Kuman, 2012).
- Pruebas de penetración: Consiste en la simulación de un ataque de los maliciosos outssiders (que no tienen un medio autorizado de acceder a los sistemas de la organización) y de maliciosos insiders (que tienen algún nivel de acceso autorizado).

El proceso implica un análisis activo del sistema en busca de posibles vulnerabilidades que podrían resultar de configuración deficiente o inadecuada del sistema, fallos de hardware o software, ya sea conocidos y desconocidos, o fallos operativos en proceso o contramedidas técnicas (Thompson, 2005).

- Pruebas pasivas: Las pruebas pasivas están diseñadas para el análisis del tráfico de telecomunicaciones. Permite detectar fallas y defectos de seguridad mediante el examen de los paquetes capturados (livetrafficor log files) (Mammar, Cavalli, & Jimenez, 2011).
- Pruebas activas: Utiliza un programador de subprocesos asignados al azar para verificar si las advertencias comunicadas por un análisis predictivo de programa son errores reales (Xiao-song Zhang, 2008).
- Fuzz testing (pruebas de caja negra): Consiste en estimular el sistema bajo prueba, utilizando datos aleatorios o mutados queridos, con el fin de detectar comportamientos no deseados como violación de confidencialidad (Xiao-song Zhang, 2008).
- Herramientas para detección de vulnerabilidad.

Las herramientas que se obtuvieron como resultado de la revisión sistemática se describen a continuación:

- QualysGuard Web Application Scanning WAS: Es una herramienta en la nube que permite realizar pruebas funcionales con selenium para aplicaciones web, además de pruebas de penetración. Permite encontrar vulnerabilidades del top 10 de OWASP (Qualys, 2014).
- WebSite Security Audit- WSSA: Permite examinar páginas web, aplicaciones y servidores web para encontrar vulnerabilidades de seguridad. Realiza pruebas de vulnerabilidades de código conocidas como: SQL Injection, XSS (Cross Site Scripting), entre otras (BeyondSecurity, 2014).

- Retina Web Security Scanner: Es una solución de escaneo de sitios web, aplicaciones web complejas para hacer frente a las vulnerabilidades de aplicaciones. Prioriza las vulnerabilidades por su nivel de riesgo (Beyontrust, 2014).
- WEBAPP 360: Enterprise Class web application scanning: Evalúa de manera completa la infraestructura de aplicaciones web, incluyendo aplicaciones web, sistemas operativos subyacentes y aplicaciones subyacentes en entorno de producción. (Tripwire, 2014).
- Frame-C: Es un software Open Source que permite analizar código fuente escrito en C. Reúne varias técnicas de análisis estático en una sola herramienta. (Frama-C, 2014).
- Parasoft C/C++ Test: Es una solución de pruebas para aplicaciones basadas en C y C++. Ayuda a desarrolladores a prevenir y eliminar defectos (Parasoft, 2014).
- Fortify Static Code Analyzer: Proporciona análisis de código estático automatizado para ayudar a los desarrolladores a eliminar las vulnerabilidades y crear software de seguridad. Analiza el código fuente, identifica las causas originarias de las vulnerabilidades de la seguridad del software y correlaciona y prioriza los resultados (HP, 2014).
- MCAfee Vulnerability Manager: Realiza monitorización activa y pasiva, además de realizar pruebas de penetración. Permite conocer los puntos en los que se debe centrar los esfuerzos de programación. Cubre las categorías de OWASP top 10 y CWE-25 (McAfee, 2014).
- Nessus Vulnerability Scanner: Permite realizar escaneo de vulnerabilidades en servidores web, servicios web, además de las vulnerabilidades de OWASP. Además de verificar la configuración erróneas del sistema y parches faltantes. Muestra informes personalizados en formato XML, CVS, PDF nativo y HTML (Tenable, 2014).

- Nexpose Vulnerability Manager: Es una solución de gestión de vulnerabilidades que combina la evaluación de vulnerabilidades y controles, la validación de vulnerabilidades y la planificación de remediación. Maneja estándares de riesgo, vulnerabilidades y gestión de la configuración como PCI DSS, NERC CIP, FISMA, entre otros (Rapid7, 2014).
- Whatweb: Identifica el sitio web, reconoce tecnologías web, incluyendo los sistemas de gestión de contenidos (CMS por sus siglas en inglés), plataformas de blog, bibliotecas de JavaScript, servidores web. También identifica los números de versiones de correo electrónico, errores de SQL y más (MorningStartSecurity, 2014).

Propuesta de trazabilidad

Finalmente, con respeto a los resultados obtenidos se realizó una matriz de trazabilidad de las herramientas utilizadas para la detección de vulnerabilidades con las técnicas, ataques y vulnerabilidades existentes: esto con el objetivo de mostrar cuales ataques y vulnerabilidades son cubiertos con que técnica y herramienta para ser mitigados. A continuación, se muestra la matriz de trazabilidad en la Tabla 2.

Tabla 2:

Matriz de trazabilidad de ataques, vulnerabilidades, técnicas y herramientas.

Ataque	Vulnerabilidad	Técnicas para detección de vulnerabilidad	Herramientas para detección de vulnerabilidades
Inyección SQL	Inyección	Análisis estático de código.	QualysGuard Web Application Scanning WAS
Ataque de fijación de sesiones	Manejo de sesión	Utilización de estándar de manejo de sesión	WebSite Security Audit-WSSA
Ataque XSS	Secuencia de comandos en sitios cruzados XSS	Análisis estático de código, pruebas de penetración.	Retina Web Security Scanner y WebSite Security Audit-WSSA
Ataque de falsificación de peticiones en sitios cruzados (CSRF)	Falsificación de peticiones en sitios cruzados (CSRF)	Análisis ético de código	QualysGuard Web Application Scanning WAS
Phising	Redirección y reenvíos no válidos.	Análisis estático de código.	SCA

Nota: Descripción del proceso de ataques y vulnerabilidades.

Como puede observarse, tras el análisis de la propuesta mostrada en la Tabla 2, la herramienta más utilizada para detección de vulnerabilidades es QualysGuard Web Application Scanning WAS, seguido de Retina Web Security Scanner y WEBAPP 360: Enterprise Class web application scanning. Así también se puede determinar que las menos utilizadas son Frame-C, Nexpose, esto debido a que son herramientas para funcionalidades más específicas.

Seguridad de la información

Conceptos

En el marco normativo de los estándares relacionados con la seguridad informática y de la información, está incluida la familia de estándares ISO/IEC 27000 e ISM3, que son normas específicas para la gestión de seguridad de la información y pueden ser aplicables a cualquier organización, independientemente de su tamaño o actividad. Otros estándares relacionados son los de calidad ISO 9001, medio ambientales como ISO 14000, de TI como el estándar CobIT y de entrega de servicios ITIL.

En este entorno empresarial, creciente y complejo es importante que las empresas tomen conciencia de aplicar continuamente una metodología de análisis de riesgo para garantizar el rendimiento de los sistemas y procesos dentro de la organización, algunas de las razones por las que las empresas deben utilizarla son:

- Permite tener claramente identificados los activos y las políticas de seguridad para que a partir de estos se puedan tomar decisiones y hacer mejoras en los procesos internos de la organización.
- Se garantiza la continuidad de negocio ya que permite tener en cuenta componentes y factores tanto internos como externos que intervienen en los objetivos misionales de la organización.
- Proporciona herramientas que permiten mitigar los riesgos a los que está expuesta la organización por medio de la creación de planes de contingencia y controles que aseguren el los sistemas de información.
- Por medio de los procesos de auditabilidad, MAGERIT permite encontrar inconsistencias dentro del sistema que no han sido identificadas y no se sospechaba de su existencia.

- Con la ayuda de las metodologías de análisis de riesgos, las empresas pueden optimizar sus procesos y obtener un retorno de inversión.

Técnicas

La norma ISO 27005 se fue acoplando con la metodología OCTAVEs a medida que se gestionaba el riesgo a la seguridad de la información al proceso Inscripciones y Admisiones. La norma ISO 27005 cuenta con 7 pasos los cuales son:

- Establecimiento del contexto
- Identificación del riesgo
- Estimación del riesgo
- Evaluación del riesgo
- Tratamiento del riesgo
- Aceptación del riesgo
- Comunicación del riesgo

La norma OCTAVEs cuenta con 3 fases las cuales son:

- Construcción de perfiles de amenazas basados en los activos.
- Identificación de las vulnerabilidades de la infraestructura.
- Desarrollo de estrategia y planes de seguridad.

Cada fase de Octaves se fue adaptando a los pasos de la norma ISO 27005. Pero antes de usar la metodología Octaves, se empezó por establecer el contexto (Establecimiento del contexto Norma ISO 27005), es decir por definir el alcance del proceso Inscripciones y Admisiones.

Normas y buenas prácticas

- **Recomendaciones de formación**

La formación es la mejor forma de concienciar a los trabajadores sobre los riesgos de seguridad, las posibles con-secuencias de incidentes y la responsabilidad de estos en los mismos, así como las principales medidas de prevención. Es por tanto fundamental que el centro de AP cuente con un plan de formación periódico, actualizado y con material estandarizado.

- **Recomendaciones de contraseña**

La composición y la privacidad de la contraseña son factores cruciales para mantener la eficacia de este mecanismo de protección frente accesos no autorizados al sistema de información sanitario. El profesional debe elegir una contraseña que cumpla las recomendaciones presentadas en pero que sea fácil de recordar aplicando alguna regla sencilla que solo él conozca.

De este modo se evita tener que anotar la contraseña para recordarla. Se pueden utilizar comprobadores de contraseña fiables para conocer el nivel de seguridad de la contraseña. La contraseña no debe aparecer ni ser compartida por ningún medio para evitar que alguien suplante su identidad.

No se debe proteger varias cuentas con la misma contraseña pues si la contraseña es descubierta, podrán suplantar la identidad del profesional en todas las cuentas.

Finalmente, la primera vez que se accede a un sitio web nunca se debe responder sí a la pregunta del navegador: ¿Desea guardar su contraseña? Si otro usuario del equipo accede de nuevo al mismo sitio web, podrá suplantar su identidad.

- **Recomendaciones de uso de certificado digital**

Un certificado digital es un conjunto de datos que permiten la identificación del titular del certificado ante terceros, intercambiar información con otras personas y entidades de manera segura, y firmar electrónicamente los datos que se envían, manteniendo su integridad y conociendo su procedencia. Su uso se está generalizando desde la entrada en vigor del DNI electrónico, y requiere una contraseña que debe ser mantenida bajo las reglas del apartado anterior.

- **Recomendaciones de uso del correo electrónico**

Como regla general, nunca se debe utilizar el correo electrónico para intercambiar datos de salud, y si fuera imprescindible, siempre debe hacerse entre cuentas corporativas de la organización de salud, firmando y cifrando los datos trasmitidos utilizando un certificado electrónico, e incluyendo una cláusula de confidencialidad advirtiendo de la naturaleza sensible de la información. Se debe evitar abrir archivos adjuntos o pinchar en enlaces recibidos a través del correo electrónico, aunque procedan de cuentas de personas conocidas.

Bajo estos archivos puede haber software malicioso (los troyanos) que acceda, controle y dañe la información del ordenador bajo una apariencia inocua, sin que sea advertido por el profesional sanitario.

- **Recomendaciones de uso y acceso a Internet e Intranet**

La visualización de un vídeo, el ingreso en un enlace encontrado en una red social, en una ventana emergente de un anuncio o tras una simple búsqueda on-line, puede poner en peligro la seguridad y la privacidad de los datos sanitarios.

Es fundamental que el trabajador esté informado de cuáles son las buenas prácticas de navegación por Internet y siga algunos consejos básicos: disponer de herramientas de seguridad (antivirus, firewall, antispam) actualizadas.

Algunas buenas practicas se puede realizar análisis con el antivirus periódicamente; no descargar ni ejecutar ningún archivo de sitios desconocidos, pues puede incluir software malicioso; nunca entregar datos persona-les o circunstancias familiares a desconocidos o en páginas no seguras (que no comiencen por https://); no aceptar contactos desconocidos en redes sociales y mensajería instantánea; nunca pulsar el botón aceptar de una ventana sin leer y entender el mensaje, y finalmente buscar un técnico informático para actualizar y configurar el navegador y el sistema operativo de forma segura.

- **Recomendaciones de uso de dispositivos extraíbles**

Conectar un dispositivo extraíble a un ordenador del centro de AP supone un riesgo alto de entrada de virus a la Intranet del centro. Para evitar infecciones, no se deben conectar dispositivos extraíbles que hayan sido utilizados en otros equipos informáticos. Hay que cifrar con un certificado digital la información que salga del centro, y cuando ya sea desechable, hacer un borrado irreversible con alguna utilidad de borrado seguro. Estas aplicaciones incluyen funciones para limpiar el área de memoria ocupada por los ficheros, con el fin de no dejar rastro de la información generada y almacenada en su ordenador durante su uso (contraseñas datos personales, etc.).

- **Recomendaciones de uso de equipos informáticos**

La medida más segura para proteger la pantalla de visualización de datos y otros periféricos cuando se ausente, es bloquear el ordenador con una contraseña. Asimismo, hay que borrar los documentos de la memoria de impresoras y fotocopiadoras utilizando las opciones de ajuste y configuración particulares de cada dispositivo. Especial precaución se debe tener al depositar ficheros en directorios o dispositivos compartidos con otros usuarios, de manera que solo accedan a la información usuarios autorizados.

En el caso de advertir alguna circunstancia en la que usuarios no autorizados puedan acceder a datos personales de salud, se debe comunicar inmediatamente al Departamento de Informática del centro de AP.

- **Recomendaciones de instalación de software**

Desconfiar del software disponible en Internet, pues suele contener software malicioso e incluso software espía que pone en riesgo los datos personales de salud.

Preferentemente, descargar software procedente de webs oficiales, utilizar un antivirus y siempre consultar antes con un técnico informático. Para disminuir riesgos, evitar la instalación de software no relacionado con el puesto de trabajo en su centro de AP.

- **Recomendaciones de incidencias de seguridad**

Es crucial concienciar a los trabajadores de la necesidad de comunicar los problemas de seguridad en el equipamiento informático del centro de AP, de manera que la organización establezca las medidas correctivas pertinentes para minimizar el impacto de las incidencias de seguridad y subsanar los daños derivados del mismo.

Capítulo III

Análisis de riesgo de OSINT

Análisis del comportamiento social en el uso de las TIC

Es importante determinar las características conocer bien cuáles son los puntos fuertes y los puntos débiles del uso de las Redes Sociales como fuente de información (OSINT). Realizaremos un análisis de la valoración mediante la herramienta DAFO, que nos ayuda a realizar una comparación para determinar un concepto específico de las TICS en el campo empresarial y social (Rahman & Esmailpour, 2016).

Tabla 3:

Análisis del uso de TICS

DAFO	EN POSITIVO	EN NEGATIVO
Aspectos Internos	○ ***Fortalezas*** - Fácil manejo. - Sirve cualquier ordenador conectado a Internet. - Complemento a otras fuentes de información.	○ ***Debilidades*** - Ignorar la información que fluye por ellas. - No conocer su funcionamiento. - Falta de tiempo. - Desconocimiento de las herramientas de monitorización.
Aspectos Externos	○ ***Oportunidades*** - Monitorización de grupos peligrosos. - Fuentes Humanas. - Detección perfiles de influencia. - Mejorar imagen. - Difundir cultura de seguridad. - Colaboración ciudadana.	○ ***Amenazas*** - Información falsa. - Infoxicación. - Movilizan gente rápidamente. - Información al instante sobre acciones que se estén llevando acabo. - Nuevos delitos. - No hay control posible de la herramienta.

Nota: Aspectos relevantes para realizar la investigación de acuerdo con un análisis de FODA

- *Fortalezas:* Las redes sociales y las herramientas gratuitas utilizadas en las TICS y asociadas a ellas no requieren de amplios conocimientos tecnológicos ni un conocimiento en específico para poder ser utilizadas en cualquier campo que lo necesite un recurso que es necesario es el tiempo y creatividad para poder aprovechar todos los beneficios que puede tener el uso de nuevas tecnologías. Esto significa que la curva de aprendizaje es relativamente rápida lo que permite empezar a obtener algunos resultados ya desde el principio.

  Es importante contar con un equipo informático complejo o equipado con accesorios difíciles de conseguir, y disponer de conexión a Internet, pues todo el trabajo OSINT en las Redes Sociales se realiza “online” (fase de obtención de información), para esto se tiene en consideración que no solo las redes sociales tienen información que se necesita, sí es cierto que puede ser una fuente muy interesante para completar conocimiento o incluso corroborar que se siguen las pistas adecuadas para la consecución de los objetivos. Por lo tanto, pueden ser consideradas como una base de datos más, que, aprovechada inteligentemente, puede servir de ayuda o apoyo en el desarrollo de las distintas investigaciones.

- *Debilidades:* Una de las principales debilidades es ignorar la información que fluye a través de las Redes Sociales donde, el investigador puede estar cerrando la puerta a la pieza vulnerable de la red informática. Generalmente no se da el valor suficiente a las redes como fuentes de información, por lo tanto, el primer paso requiere de la construcción de una visión global. El problema para conseguirlo, son casos que se atraviesan momentos de incertidumbre que pueden llevar al abandono lo cual determina en ataques o vulnerabilidades de la seguridad, una de las claves para evitarlo, es la información básica de las redes sociales, se enmarca dentro de la fase de obtención de información

Del conocido ciclo de Inteligencia y el problema es que es una de las fases que más tiempo requiere. Por último, parte de la información se obtendrá de un análisis previo facilitado en la mayoría de las ocasiones por herramientas específicas.

- *Oportunidades*: En la actualidad todo movimiento, grupos radicales, tienen presencia en las redes sociales con la intención de difundir su ideología, realizar captación de nuevos miembros, explicar su agenda e influir en conductas. Por ejemplo, en 2008, Facebook se vio empujada a expulsar de su plataforma a varios grupos de neonazis que hacían apología de racismo.

Por otro lado, a día de hoy podemos leer las actividades de Anonymous a través de su propio Twitter donde informan de sus operaciones y sus logros. Por último, incluso grupos radicales marroquíes que luchan por Ceuta y Melilla, convocan manifestaciones y acciones a través de grupos en Facebook como el de “Libertad para Ceuta y Melilla”. Información pública que puede ser de mucha utilidad para las investigaciones de las Fuerzas y Cuerpos de Seguridad del Estado. Por otro lado, la base de una Red Social son las relaciones humanas, lo que hace de este medio un campo fértil para todo lo relacionado con la HUMINT.

Ya no sólo facilitando el acceso a través de perfiles adaptados a los grupos de los que se desea obtener información, sino que también redes como LinkedIN pueden ayudar al investigador a conocer la existencia de expertos en determinadas materias. Hoy por hoy, la detección de perfiles de influencia, por ejemplo en Twitter, es fundamental para conocer quién o quiénes son los promotores de determinada iniciativa, como pudiera ser el caso de incitaciones a cometer actos de violencia.

Conocer estos perfiles permite hacer un seguimiento a toda la red, adelantándose, por ejemplo, a posibles actuaciones no autorizadas o situaciones de riesgo.

Ya desde el punto de la difusión, el hecho de tener presencia en las Redes Sociales permite mejorar la imagen de la organización, así como educar y sensibilizar a la ciudadanía en la cultura de seguridad a través de mensajes que recuerden que la seguridad es cosa de todos. Por último, se pueden llevar a cabo también acciones muy novedosas como permitir a los ciudadanos que se expresen y que ayuden a las FFCC de Seguridad del Estado.

Aunque de momento estas acciones están teniendo baja acogida, son una línea a tratar que requiere además de una concienciación y cambio de cultura en proceso.

- *Amenazas:* Dos de las principales amenazas del uso de la información de las redes sociales como fuente de investigación son la información falsa y la infoxicación (Situación de exceso informacional, en la que tienes más información para procesar de la que humanamente puedes).

  Por la Red fluye todo tipo de información sin filtrar, que salvo en países determinados en donde se aplica censura (como China o India). Puesto que cualquiera que tenga un perfilen una red social puede empezar a difundir lo que quiera sin control, se debe tener especial cuidado en la valoración del contenido y de la fuente, pues hoy por hoy también se ejercen acciones de desinformación.

  En cuanto a la infoxicación, debemos tener en cuenta que las Redes Sociales están plagadas de ruido. El ruido no es más que información inútil que dificulta la obtención de la información realmente relevante y que necesitamos. Para contrarrestar la infoxicación, existen una serie de herramientas como por ejemplo las indicaciones de contenidos y que es extensible no sólo a la Red, sino también a la Red Social. Desde un punto de vista más operativo, las Redes Sociales pueden llegar a movilizar rápidamente a grandes cantidades de personas, con los problemas de seguridad que ello puede generar, asociados a toda concentración masiva.

Es por ello por lo que conviene atender sus contenidos, con objeto finalmente de garantizar la seguridad de todos los ciudadanos. Por otro lado, a través de las Redes, los ciudadanos se avisan con rapidez también contra acciones que puedan estar llevando a cabo las FFCC de seguridad. Esto significa que las operaciones en calle alcanzan un nuevo nivel del concepto de “públicas”.

Entre ellas está el riesgo de grabaciones de vídeo que pueden ser subidas al instante a YouTube exponiendo públicamente a los operativos. Por otro lado, se han estado utilizando con frecuencia para dificultar desahucios o para impedir la identificación de inmigrantes. Desgraciadamente, las Redes Sociales, como herramienta de comunicación también son utilizadas para cometer delitos. Por ejemplo, en distintos países empiezan a ser frecuentes los casos de robos en casas vacías derivados de que alguno de los miembros de la familia publicaba en Facebook que se iban de vacaciones.

También exponen a los “navegantes” a estafas, delitos informáticos, etc. Por último, otra de las principales amenazas es la imposibilidad de controlar la herramienta. Estas herramientas están en manos de grandes corporaciones que definen sus propios objetivos y necesidades. Obtener respuesta de estas corporaciones es muy complicado y en absoluto inmediato. Por ejemplo, Brasil está en trámites de juicio con Twitter por no borrar mensajes que avisan de dónde están los controles de tráfico.

Por lo tanto, sólo se puede observar y en el mejor de los casos interactuar “como uno más” para tratar de influir, por ejemplo, educando contra ciertos riesgos.

Metodología

OCTAVE es un estudio auto dirigido, desarrollado por un equipo interdisciplinario llamado el equipo de análisis, el cual se compone de personas de las áreas de negocio y del área de TI.

Esta composición se explica con el hecho de que los funcionarios del negocio son los más indicados para identificar qué información es importante en los procesos del día a día y cómo se usa dicha información; por su parte, son las personas del área de TI las que conocen los detalles de configuración de la infraestructura y las debilidades que puede tener.

Estos dos puntos de vista son importantes para tener una visión global de los riesgos de seguridad de los servicios de TI. El equipo de análisis debe identificar los activos relacionados con la información que son de importancia para la organización, entendiendo esta importancia en términos de que se garantice la continuidad de operación.

El análisis se focaliza sobre los activos que se identifican como críticos y la identificación del modo en que se relacionan dichos activos entre sí, las amenazas a las que están expuestos y las vulnerabilidades (organizacionales y tecnológicas).

El estudio se hace desde un punto de vista operacional, se verifica cómo se usan los diferentes activos y cómo pueden estar en riesgo debido a amenazas de seguridad. Finalmente, se define una estrategia basada en prácticas para el mejoramiento organizacional y un plan de mitigación para reducir el riesgo al que está expuesta la organización.

Proceso general

OCTAVE se desarrolla mediante una serie de talleres en los que el equipo de análisis y el personal clave de los diferentes niveles de la organización adelantan el levantamiento y análisis de la información. Este proceso se divide en tres fases:

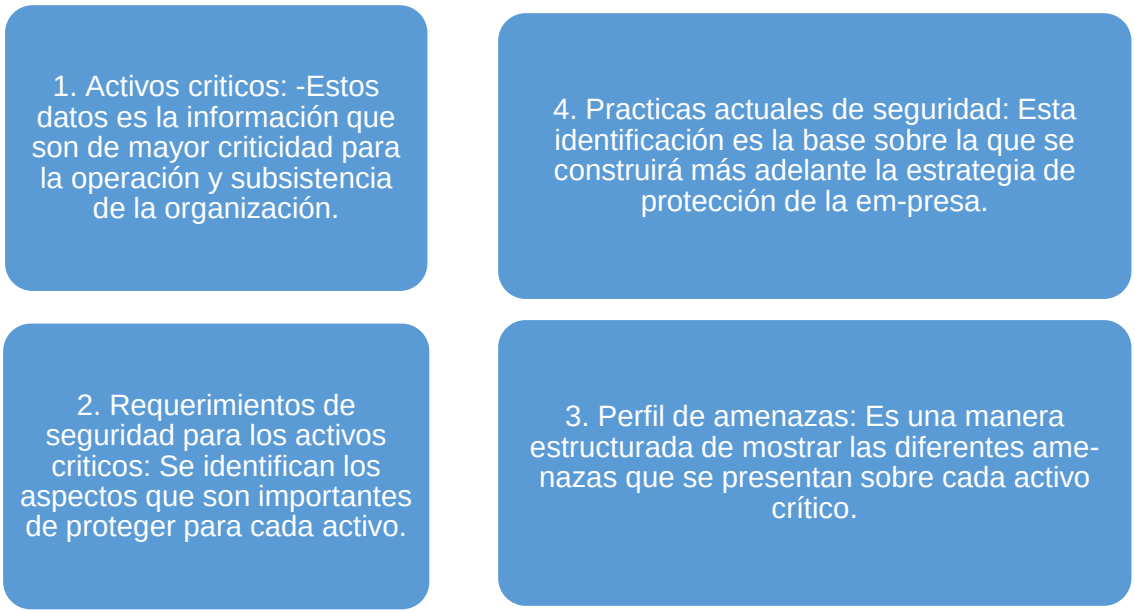
- Fase 1- Identificación: Construir perfiles de amenazas basados en los activos. Los diferentes miembros de la organización contribuyen con su visión sobre los activos que son críticos para la empresa, la manera como se usan y lo que en la actualidad se está

haciendo para protegerlos. El equipo evalúa la información y selecciona los activos más importantes.

A continuación, se describen los requerimientos de seguridad y se crea un perfil de amenazas para cada activo crítico.

Figura 5:

Resultados de la fase de identificación.

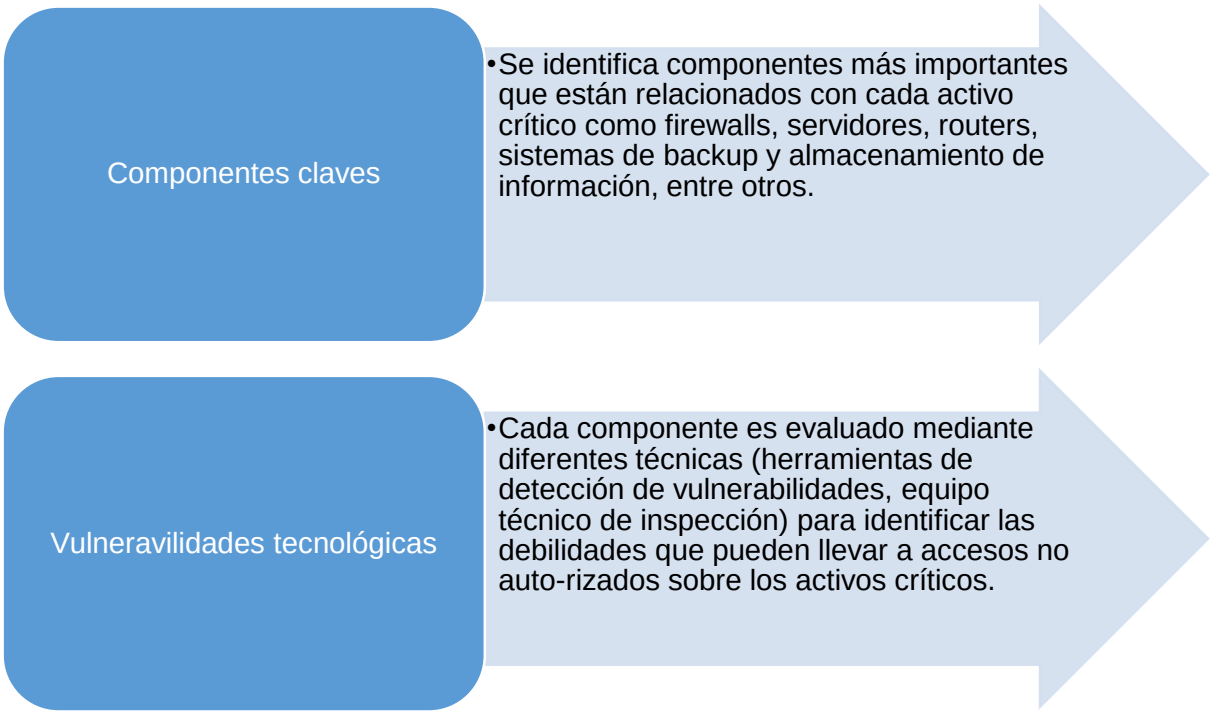


Nota: Resultados de la fase de identificación.

- Fase 2- Valoración: Identificar vulnerabilidades en la infraestructura El equipo de análisis identifica los principales elementos de TI y los diferentes componentes que se relacionan con cada activo crítico. Se evalúan entonces los diferentes componentes para identificar las vulnerabilidades que pudieran facilitar las acciones no autorizadas sobre los activos críticos. Las salidas de esta fase son, entre otras:

Figura 6:

Salida de la fase de valoración.

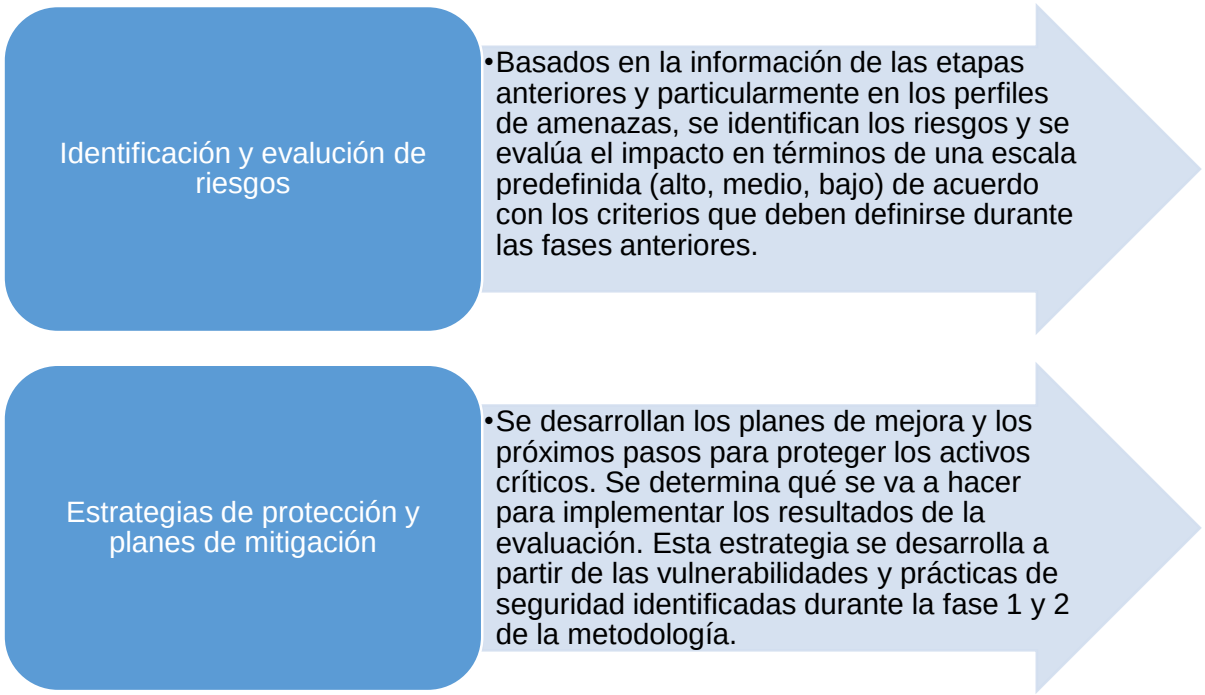


Nota: Resultados de la fase de valoración.

- Fase 3- Tratamiento: Desarrollar estrategias y planes de seguridad. En esta etapa de riesgos sobre los diferentes activos críticos y decide qué acciones tomar. El equipo crea entonces una estrategia de protección y planes de mitigación, basados en la información recolectada. Las salidas de esta fase son:

Figura 7:

Salida de la fase de tratamiento.



Nota: Resultados de la fase de tratamiento.

Alcance de análisis del riego

El análisis de riesgo se determinara en las pequeñas empresas lo que está relacionado con las TICS y también determinando el proceso y rol que efectúan los involucrados en la empresa tanto como personas internas en el negocio como externas, de esta manera podríamos determinar características de análisis donde a continuación se detallan enfocados en campos de la empresa que pueden ser vulnerables con mayor frecuencia:

Formas de pago

- Información de los clientes y proveedores
- Información de la empresa de manera interna y externa
- Comportamientos con medios tecnológicos

Al determinar este proceso de cuáles serán segregados para una valoración un análisis más profundo con el fin de determinar los datos importantes con OSINT que se pueden recaudar ya que al manejar las fuentes abiertas los datos son accesibles para cualquier usuario que realice las búsquedas que necesita de la víctima. Se determina el análisis de los riegos al agrupar un ejemplo de mayor trascendencia en diferentes campos de mitigación con criterios de inseguridad que OSINT puede proporcionar los cuales pueden ser:

- Pérdida de identidad
- Espionaje en las redes
- Pérdidas económicas empresariales y personales
- Contaminación de equipos tecnológicos

Identificación

Para la identificación de los riegos determinaremos algunos procesos lo cual nos permita identificar varios parámetro en donde OSINT afecta de manera directa a la seguridad de las TICS determinando amenazas y vulnerabilidades en algunos aspectos, en esta parte del proceso de gestión de riesgos en la que conocemos e inspeccionamos los riesgos.

El objetivo de la identificación del riesgo es conocer los sucesos que se pueden producir en la organización y las consecuencias que puedan tener sobre los objetivos de la empresa. Determinando algún aspecto los cuales se detallan a continuación:

- Amenazas
- Vulnerabilidades
- Definición del riesgo

Amenazas

Las amenazas que se desarrollan en nuestro entorno se pueden especificar y determinar en algunos camos uno de ellos es en las empresas o medios de cotidianidad como son las areas de trabajo y procesos cotidianos que se realizan a continucaion se deteminan amenazas que se pueden ver en disctintos campos en un medio cotidiano de distintos enfoques de activos en el campo tecnológico.

Tabla 4:

Descripción de amenazas

Amenaza	Descripción	Activo	Campo y causa
Alteración de Datos	Las empresas se encuentran amenazados por recibir o dar información que ha sido alterada donde podemos determinar este caso de manera frecuente es en el área de recursos humanos ya que es información que se solicita es personal.	Software	Información de la empresa de manera interna y externa y la causa es el bajo nivel de seguridad a la base de datos
Hacker	Los hacker necesitan es información que les ayude a determinar un blanco donde poder determinar los ataques las bases de datos es el punto que buscan información y como seria en una empresa los datos e información económica de los clientes y proveedores	Servidores	Información de los clientes y proveedores su causa puertos abiertos innecesarios
Fraude interno	Los fraudes internos llevados a cabo por personal relacionado con el área tecnológica y quien tenga a accesos a estas fuentes por lo general son datos vulnerados o modificaos para fines de estafa.	Sistema Contable	Formas de pago su causa falta de incentivos a los empleados o involucrados
Virus	Afectación de equipos donde se maneja información sensible los cuales pueden ser equipos móviles o estáticos.	Antivitus	Equipos causa falta de seguridad y desconocimiento de buenas practicas
Daños de Hardware	Interrupción de red para procesos específicos, empresa o medio de comunicación	Equipos tecnológicos	Comportamientos con medios tecnológicos

Nota: Detalle de las amenazas con las que se mitigo la investigación.

Vulnerabilidades

Las vulnerabilidades se desarrollan de manera que podamos determinar con las mismas amenazas ya descritas con el fin de determinar cuál sería el proceso ya que estas se llevan a cabo con fuentes abiertas.

Tabla 5:

Descripción de vulnerabilidades

Amenaza	**Vulnerabilidades**	**Técnica de detección**
Alteración de Datos	Suplantación de identidad Documentación fraudulenta Facilidad de obtención de información de entidades publicas Cambio de números de identificación Certificados alterados Falsificación de firmas.	Análisis estático de procesos en el sistema
Hacker	Contraseñas común mente utilizadas Puertos no utilizados y habilitados Utilizar navegadores donde guarda direcciones IP Cámaras de seguridad Seguridad de base de datos	Utilización de estándares de manejo se sesiones
Fraude interno	Evasión de impuestos Perdida de información contable Suplantación de valores contables Declaraciones excesivas Pagos indebidos de recursos humanos Duplicidad de contabilidad Coimas dentro de entidades asociadas a lo contable	Pruebas de penetración al sistema.
Virus	Dispositivos de almacenamiento infectados Conexión a Internet sin contar con recomendaciones de navegación. Ingreso a páginas con alto grado de malware. Ingreso a correos con contenido desconocido. Uso indebido de redes sociales No utilizar licencias de aplicaciones y programas	Análisis estático de procesos en el sistema
Daños de Hardware	Daños con el polvo Humedad en los dispositivos tecnológicos Uso de dispositivos genéricos Malas instalaciones donde están los equipos	

Nota: Detalle de las vulnerabilidades con las que se mitigo la investigación.

Las técnicas de detección nos permiten determinar los puntos de vulnerabilidad donde se obtiene con mayor frecuencia los puntos de ataques y provocar de esta manera las amenazas.

- Pruebas de penetración al sistema: Consiste en la simulación de un ataque de los maliciosos outssiders (que no tienen un medio autorizado de acceder a los sistemas de la organización) y de maliciosos insiders (que tienen algún nivel de acceso autorizado).
- El proceso implica un análisis activo del sistema en busca de posibles vulnerabilidades que podrían resultar de configuración deficiente o inadecuada del sistema, fallos de hardware o software, ya sea conocidos y desconocidos, o fallos operativos en proceso o contramedidas técnicas (Thompson, 2005).
- Análisis estático de procesos en el sistema o (auditoria de código fuente): Es un método en el que no se requiere ejecutar el programa, este realiza un análisis de código fuente directo para determinar huecos en la seguridad (Sreenivasa & Kuman, 2012).
- Utilización de estándares de manejo se sesiones: Estos estadales son métodos de buenas prácticas para evitar la vulnerabilidad de contraseñas de todos los procesos que tengan esta consideración cualquier tipo de identificación como seguridad las mismas que sean contraseñas reconocimiento facial o detección de huellas.

Definición de riesgos

Los riesgos se definen mediante el análisis de las amenazas y vulnerabilidades que se determinaron en el análisis anterior a continuación se detallen.

- Alteración de Datos

Problemas legales a los que se puede ver expuesta la empresa si se constata que tiene alteración de datos. Si el caso se da al tratar obtener trabajo y se constante que los datos son inconsistentes tiene el riesgo que no le den el trabajo.

Al realiza una suplantación de identidad los riesgos son varios ya que pueden ser legales o llevar a casos extremos como perder la vida ya que hay intereses fuertes cuando asumen estos riesgos. La suplantación de identidad también es un método de salvaguardar la integridad de una persona ya que en casos legales donde se necesita testigos protegidos se suplanta o simplemente se oculta la identidad de estas personas.

- Hacker

Se lleva a cabo el control de base de datos mediante la vulnerabilidad de contraseñas comunes o al no tener conocimiento de buenas prácticas al determinar una contraseña que se proteja. La ingeniería social es una de las vulnerabilidades que provocan uno de los mayores riesgos ya que mediante el análisis de las victimas llevan a cabo el analizar e investigar sus aspectos relevantes para el ataque.

- Fraude interno

Demandas por el estado por evasión de impuestos o ilegalidad de documentación donde corre el riesgo de perder la empresa o ser portador de una multa sustanciosa donde puede llevar a la quiebre la empresa. Robo de dinero en la empresa con procesos que se altera la documentación o valores de la empresa corre el riesgo de pérdida de trabajo procesos legales donde los causantes sean expuestos.

- Virus

Falta de protección del software pérdida de información en los ordenadores que no tienen la protección de n antivirus. Mal funcionamiento del quipo por no tener licencias de las aplicaciones y software pagados esto determina un riego de perdida de información y que sea vulnerable a ataques con virus.

Páginas web son las utilizadas para la propagación de virus ya que muchas veces son vinculadas a páginas externas que al abrir la página requerida se abren automáticamente y de esta manera infectan al equipo con virus

- Daños de Hardware

Equipos dañados por contaminación ambiental siendo esto un caso de riesgo de manera directa ya que el equipo dejaría de funcionar. Los equipos sometidos a la humedad muchas veces corren el riesgo de no tener reparación por lo cual se debería realizar la adquisición de un nuevo equipo siendo un casto alto para la empresa.

Valoración

Escala de valoración

Para las escalas de valoración determinaremos para el impacto y la probabilidad que serán los parámetros de evaluación de los riesgos. Referente a la tabla de impacto se especificara la valoración determinando los casos que se describirá en cada nivel de afectación. En la tabla 3 se aclara la clasificación del nivel de impacto que pueden tener las amenazas sobre los activos de la organización.

Tabla 6:

Valoración del impacto

Tabla de impacto			
Valoración			**Descripción**
A	Alta	3	La ejecución de las vulnerabilidades a) Causar una alta pérdida económica de los principales activos tangible y recursos. b) Puede significativamente violar dañar impedir alcanzar recaudaciones o intereses. c)Puede causar la muerte humana o lesiones graves
M	Media	2	La ejecución de las vulnerabilidades a)Causar una alta pérdida económica de los principales activos tangible y recursos b)Puede significativamente violar dañar impedir alcanzar recaudaciones o intereses c) Puede causar lesiones personales o emocionales.
B	Baja	1	La ejecución de las vulnerabilidades a)Causar una alta pérdida económica de los principales activos tangible y recursos b)Puede significativamente violar dañar impedir alcanzar recaudaciones o intereses

Nota: Detalle del impacto con las que se mitigo la investigación.

Referente a la tabla de valoración de la probabilidad se obtienen los índices (Alta, media, baja) para medir la ocurrencia de algún evento que represente un riesgo para la organización y la escala de valoración de ese riesgo, tal y como se muestra en la tabla siguiente.

Tabla 7:
Valoración de la probabilidad

Valoración			Eventos	Riesgos
A	Alta	3	La fuente de amenazas es altamente motivada y suficientemente capaz de ser ejecutada y los controles para prevenir esta probabilidad son realizado pero no efectivos	Si se evalúa un riesgo como alto existe la necesidad correctiva. Un sistema de información puede continuar operando pero el plan de acciones correctivas debe ser puesto en práctica tan pronto como sea posible.
M	Media	2	La fuente de amenaza es motivada y capaz pero los controles aplicados pueden dificultar la ejecución exitosa de la vulnerabilidad.	Si se evalúa un riesgo como medio acciones correctivas son necesarias y un plan debe ser desarrollado para incorporar estas acciones en un periodo razonable de tiempo
B	Baja	1	La fuente de amenaza es mínimamente motivada existe controles relacionados para prevenir las amenazas existe dificultada para la ejecución de la vulnerabilidad	Si un riesgo se evalúa como bajo se debe determinar acciones de acuerdo con las necesidades y la obtención de un nivel de riego aceptable.

Nota: Detalle de la probabilidad con las que se mitigo la investigación.

Después de determinar la valoración podemos estipular parámetros en los riesgos expuestos donde determinaremos los riesgos que se determinan con OSINT.

Nivel aceptable del riesgo

El nivel aceptable del riesgo lo tomaremos en consideración respecto a los riesgos y la valoración de los riesgos donde se especificara los datos que se obtuvo con respecto a los riesgos expuestos y determinando que el análisis se da mediante la PROBABILIAD por el IMPACTO (P*I) determinando el nivel de riesgo (NR) donde la formula se efectúa de la siguiente manera NR=P*I.

El nivel de aceptación se determina en una valoración de (3*2= 6) con respecto a los datos proporcionados en un análisis de riesgo.

Tabla 8:

Tabla de análisis de riesgos

	Riesgo	Niveles		
		Probabilidad	Impacto	Total
1	Problemas legales a los que se puede ver expuesta la empresa si se constata que tiene alteración de datos.	2	2	4
2	Si el caso se da al tratar obtener trabajo y se constante que los datos son inconsistentes tiene el riesgo que no le den el trabajo.	1	2	2
3	Al realiza una suplantación de identidad los riesgos son varios ya que pueden ser legales o llevar a casos extremos como perder la vida ya que hay intereses fuertes cuando asumen estos riesgos.	3	3	9
4	La suplantación de identidad también es un método de salvaguardar la integridad de una persona ya que en casos legales donde se necesita testigos protegidos se suplanta o simplemente se oculta la identidad de estas personas.	1	3	3
5	Se lleva a cado el control de base de datos mediante la vulnerabilidad de contraseñas comunes o al no tener conocimiento de buenas prácticas al determinar una contraseña que se proteja	2	3	6
6	La ingeniería social es una de las vulnerabilidades que provocan uno de los mayores riesgos ya que mediante el análisis de las victimas llevan a cabo el analizar e investigar sus aspectos relevantes para el ataque.	3	3	9
7	Demandas por el estado por evasión de impuestos o ilegalidad de documentación donde corre el riesgo de perder la empresa o ser portador de una multa sustanciosa donde puede llevar a la quiebre la empresa.	2	1	2
8	Robo de dinero en la empresa con procesos que se altera la documentación o valores de la empresa corre el riesgo de pérdida de trabajo procesos legales donde los causantes sean expuestos.	1	2	2
9	Falta de protección del software pérdida de información en los ordenadores que no tienen la protección de antivirus	3	2	6
10	Mal funcionamiento del quipo por no tener licencias de las aplicaciones y software pagados esto determina un riego de perdida de información y que sea vulnerable a ataques con virus.	3	1	3
11	Páginas web son las utilizadas para la propagación de virus ya que muchas veces son vinculadas a páginas externas que al abrir la página requerida se abren automáticamente y de esta manera infectan al equipo con virus	3	3	9
12	Equipos dañados por contaminación ambiental siendo esto un caso de riesgo de manera directa ya que el equipo dejaría de funcionar.	2	3	6
13	Los equipos sometidos a la humedad muchas veces corren el riesgo de no tener reparación por lo cual se debería realizar la adquisición de un nuevo equipo siendo un casto alto para la empresa.	1	3	3

Nota: Detalle para el análisis de la investigación.

El análisis de estos riesgos nos determina un criterio sobre los datos efectuados sobre la probabilidad y el impacto.

Probabilidad

La probabilidad de ocurrencia de que las amenazas se puedan desarrollar con las vulnerabilidades ya descritas lo que se pudo determinar en el análisis de estos riesgos de manera general tomaremos en consideración.

Los riesgos con una incidencia fuera del nivel de tolerancia de, lo cual detallaremos y explicaremos a continuación el riesgo con la mayor probabilidad de ocurrencia.

Tabla 9:

Análisis de riesgo con mayor probabilidad

		Niveles		
	Riesgo	**Probabilidad**	**Impacto**	**Total**
3	Al realiza una suplantación de identidad los riesgos son varios ya que pueden ser legales o llevar a casos extremos como perder la vida ya que hay intereses fuertes cuando asumen estos riesgos.	3	3	9
6	La ingeniería social es una de las vulnerabilidades que provocan uno de los mayores riesgos ya que mediante el análisis de las victimas llevan a cabo el analizar e investigar sus aspectos relevantes para el ataque.	3	3	9
9	Falta de protección del software pérdida de información en los ordenadores que no tienen la protección de antivirus	3	2	6
10	Mal funcionamiento del quipo por no tener licencias de las aplicaciones y software pagados esto determina un riego de perdida de información y que sea vulnerable a ataques con virus.	3	1	3
11	Páginas web son las utilizadas para la propagación de virus ya que muchas veces son vinculadas a páginas externas que al abrir la página requerida se abren automáticamente y de esta manera infectan al equipo con virus	3	3	9

Nota: Detalle de la probabilidad con mayor incidencia.

La probabilidad con mayor incidencia se determina en los riegos cuando existe suplantación de identidad ya que análisis de riesgos pueden llevar a casos extremos como ser problemas legales o muchas veces hasta perdida de la vida.

Otro de los riesgos que se toman en consideración como de mayor probabilidad de ocurrencia son los que se dan por ingeniería social donde los puntos de vulnerabilidad los determina el usuario ya que puede ser víctima por su misma información descrita en varios medios como las redes sociales que son aspectos que son los principales medios que OSINT toma para realizar la investigación ya que son los menos seguros y de obtención de datos más frecuentes.

Donde existe una mayor incidencia de probabilidad es en el campo de Virus ya que los riesgos determinados existe una alta puntuación de probabilidad de ocurrencia ya que las vulnerabilidades son expuestas y con mayor accesibilidad por falta de licencias y seguridades en

el software hace que el equipo tecnológico sea inseguro y vulnerable determinando mal funcionamiento de equipos y pedida de información, también se encuentran las páginas web que muchas veces por falta de conocimiento no se toman datos ni se determinan parámetros para el uso de buenas prácticas en el uso del Internet.

Impacto

El impacto del riesgo donde se terminó en mayor frecuencia es en los siguientes riesgos, lo cual pertenece a un análisis que cubre un impacto empresarial y social en los aspectos descritos a continuación.

Tabla 10:

Análisis de riesgo con mayor impacto

		Niveles		
	Riesgo	**Probabilidad**	**Impacto**	**Total**
3	Al realiza una suplantación de identidad los riesgos son varios ya que pueden ser legales o llevar a casos extremos como perder la vida ya que hay intereses fuertes cuando asumen estos riesgos.	3	2.6	7.8
4	La suplantación de identidad también es un método de salvaguardar la integridad de una persona ya que en casos legales donde se necesita testigos protegidos se suplanta o simplemente se oculta la identidad de estas personas.	1.7	3	5.1
5	Se lleva a cado el control de base de datos mediante la vulnerabilidad de contraseñas comunes o al no tener conocimiento de buenas prácticas al determinar una contraseña que se proteja	2	2.6	5.2
6	La ingeniería social es una de las vulnerabilidades que provocan uno de los mayores riesgos ya que mediante el análisis de las victimas llevan a cabo el analizar e investigar sus aspectos relevantes para el ataque.	2.8	2.8	7.84
11	Páginas web son las utilizadas para la propagación de virus ya que muchas veces son vinculadas a páginas externas que al abrir la página requerida se abren automáticamente y de esta manera infectan al equipo con virus	3	3	9
12	Equipos dañados por contaminación ambiental siendo esto un caso de riesgo de manera directa ya que el equipo dejaría de funcionar.	2	2.9	5.8
13	Los equipos sometidos a la humedad muchas veces corren el riesgo de no tener reparación por lo cual se debería realizar la adquisición de un nuevo equipo siendo un casto alto para la empresa.	1	3	3

Nota: Detalle del impacto con mayor incidencia.

El impacto con mayor ocurrencia se determina en el campo de Hackers ya que los parámetros y procesos de vulnerabilidad son expuestos y con mayor frecuencia determinados al ataque de un objetivo con fines de índole destructivo o de estafa.

Donde se puede evidenciar que las aplicaciones, bases de datos entre otros puntos que en el campo de hacker se da es importante determinar que las vulnerabilidades de estos puntos también son utilizados de manera de salvaguardar la integridad y privacidad.

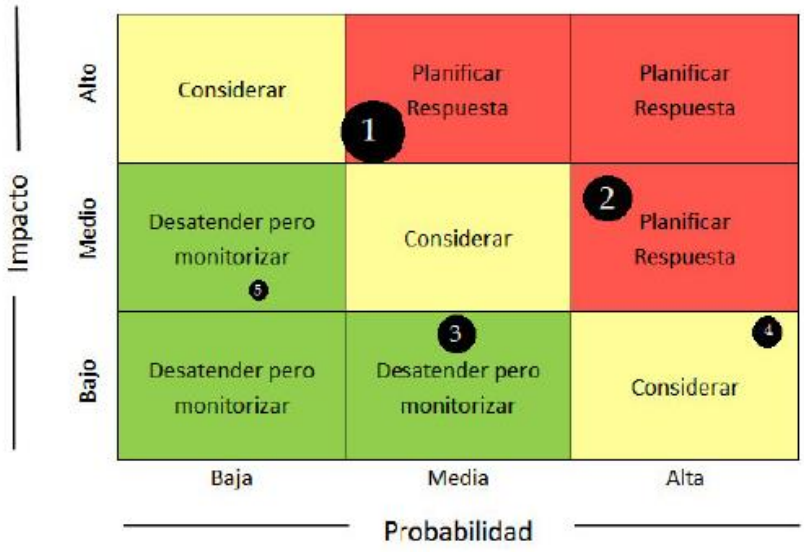
El impacto que la ingeniería social en la actualidad nos da parámetros de investigación y de indagación de información ya que estos ataques son conocidos de manera de engaño para la victima de manera que proporcione la información necesaria para que se pueda visualizar y realizar los objetivos de los atacantes.

Mapa de riego

Al realizar el grafico podemos determinar el riesgo de acuerdo a su equivalencia donde podemos determinar los niveles de riesgos a los que están inmersas las diferentes amenazas y las vulnerabilidades a la que pueden ser expuestas.

Figura 8:

Análisis de valores de mapa de riesgos.

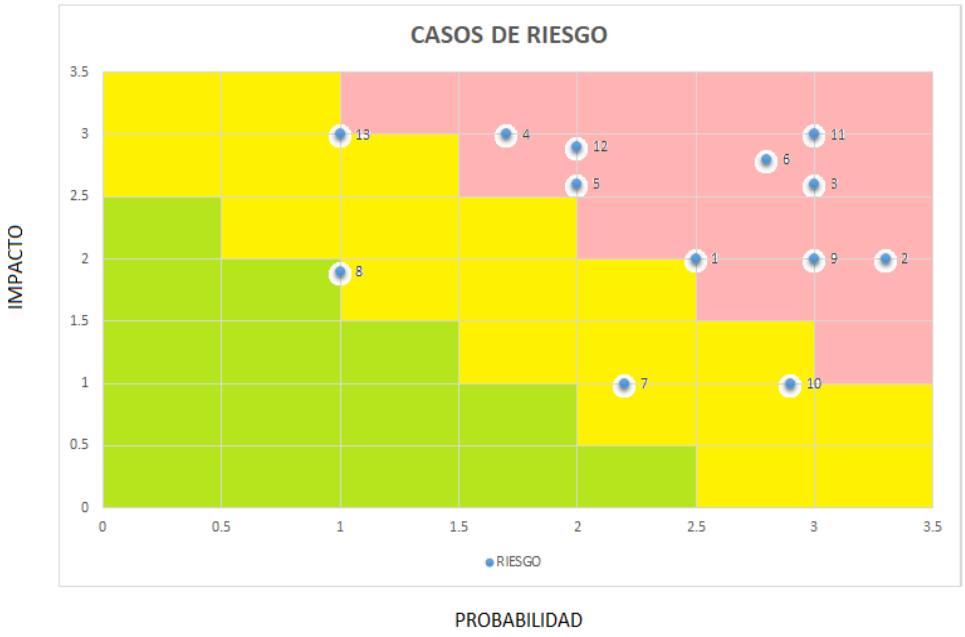


Nota: Detalle de los valores de riesgo de la investigación.(Alzoubaidi, 2016)

Donde se determina valores y consistencias que se tiene en el planteamiento del mapa, a continuación se desarrolla el mapa de riesgos para realizar el análisis mediante los puntos que están inmersos en los datos ya analizados anteriormente.

Figura 9:

Análisis de riesgo de la investigación con especificación del mapa.



Nota: Detalle del mapa de riesgos de la investigación con sus parámetros establecidos.

Podemos determinar que los riesgos que están puestos en consideración sin que tengan un efecto relativo en la sociedad son los siguientes (1, 8, 7, 10, 13) son estipulados con riesgos de un impacto y probabilidad que se puede solventar donde se podría a

Aplicar de manera general un posible análisis.

Donde el impacto puede ser:

- Causar una alta pérdida económica de los principales activos tangible y recursos
- Puede significativamente violar dañar impedir alcanzar recaudaciones o intereses

- Puede causar lesiones personales o emocionales.

Respecto al análisis de las probabilidades se puede determinar

La fuente de amenaza es motivada y capaz pero los controles aplicados pueden dificultar la ejecución exitosa de la vulnerabilidad.

Si se evalúa un riesgo como medio, acciones, correctivas son necesarias y un plan debe ser desarrollado para incorporar estas acciones en un periodo razonable de tiempo

En el siguiente parámetro a analizar están los riegos que necesitan la planificación de respuestas inmediatas los riesgos son los siguientes (2, 3, 4, 5, 6, 9, 11, 12) son estipulados con riesgos de un impacto y probabilidad que necesitan acciones inmediatas ya que su ponderación es alta.

Donde el impacto puede ser:

- Causar una alta pérdida económica de los principales activos tangible y recursos
- Puede significativamente violar dañar impedir alcanzar recaudaciones o intereses
- Puede causar la muerte humana o lesiones graves

Respecto al análisis de las probabilidades se puede determinar:

La fuente de amenazas es altamente motivada y suficientemente capaz de ser ejecutada y los controles para prevenir esta probabilidad son realizado pero no efectivos.

Si se evalúa un riesgo como alto existe la necesidad correctiva. Un sistema de información puede continuar operando pero el plan de acciones correctivas debe ser puesto en práctica tan pronto como sea posible.

Capítulo IV

Tratamiento

Para el tratamiento de los riesgos Las tendencias de la seguridad de la información se han convertido en la parte esencial de las empresas, convirtiéndose la información en el activo más relevante, el cual requiere la atención de todos los que tienen acceso a la misma. El componente humano continúa siendo una pieza crítica en la gestión de seguridad de la información en las empresas, la gran mayoría de iniciativas recae en el ámbito estratégico y táctico (Bhattacharya et al., 2018).

“Una empresa es una unidad institucional considerada como productora de bienes y servicios.” (SCN, 2008). Como agente económico con autonomía, puede adoptar decisiones financieras y de inversión con autoridad y responsabilidad para asignar recursos a la producción de bienes y servicios y puede realizar una o varias actividades productivas.

La forma de organización de las empresas debe estar cubierta por un sistema de seguridad informática, de esta manera se salvaguarda el acceso a la información o modificación de la misma, permitiendo que solo personas autorizadas puedan plegarse (Bhattacharya et al., 2018)

Los principales objetivos de la seguridad informática en las empresas por tanto son:

- Detectar los posibles problemas y amenazas a la seguridad, minimizando y gestionando los riesgos.
- Garantizar la adecuada utilización de los recursos y de las aplicaciones de los sistemas.
- Limitar las pérdidas y conseguir la adecuada recuperación del sistema en caso de un incidente de seguridad.
- Cumplir con el marco legal y con los requisitos a nivel organizativo.

Es menester además la fiabilidad en el comportamiento del sistema de seguridad, lo cual conlleva a tener en cuenta tres aspectos: la confidencialidad, que no es más que la privacidad de la información del sistema, así, solo puede ser leída por quien se encuentre acreditado a hacerlo. La integridad, que permite corroborar que no ha existido alteración en la documentación empresarial finalmente, la disponibilidad.

La facultad de hacer que la información sea accesible a los usuarios en el momento que sea notoria su necesidad, restando impedimentos por bloqueos o pérdidas (Peddi et al., 2015). Se puede asegurar, que la información es un activo con valor para el curso de las actividades empresariales, en este caso, estaríamos hablando de seguridad de la información, es decir, la protección de la integridad, disponibilidad y confidencialidad de la información, dependiendo de lo demandado para cumplir las metas de la empresa (Peddi et al., 2015)

Estrategias de tratamiento

Las estrategias de tratamiento son ponderadas y descritas en parámetros de ISO2700 y COBIT para el uso de buenas prácticas de seguridad informática, algunas de las cuales son descritas a continuación:

- COBIT:

Es el proceso de auditoría de sistemas donde sus parámetros conllevan a proveer seguridad informática sus principales características son:

  - Satisfacer las necesidades del accionista.
  - Considerar la empresa de punta a punta.
  - Aplicar un´único modelo de referencia integrado.
  - Posibilitar un enfoque holístico
  - Separar gobierno de la gestión.

Uno de los propósitos por lo cual se desarrolló el sistema COBIT, fue para facilitar y ayudar a las organizaciones obtener el valor óptimo de la tecnología de la información conservando el balance entre la realización de beneficios, la utilización de recursos y los fases de riesgo asumidos. COBIT 5 posibilita que la tecnología de la información sea manejada y gestionada de forma conceptual para toda la organización, teniendo en cuenta el negocio, o empresa y sus principales y funcionales de punta a punta as´ı como los interesados internos y externos.

Este sistema se puede utilizar y aplicar en organizaciones de diferentes tipos y todos los tamaños, sin importar el sector de desarrollo de la empresa puede ser privado, publico entidades sin fines de lucro (Julio Jhovany Santacruz Espinoza, 14 de Diciembre de 2017).

- ISO27000:

La norma ISO 27000 es certificable. Esto significa que una empresa puede solicitar una auditoría a una entidad certificadora acreditada y si la supera, obtener la certificación. Antes de solicitar la auditoría las empresas necesitan contar con un Sistema de Gestión de Seguridad de la Información (SGSI). El SGSI debe estar implementado en la empresa como mínimo con tres meses de antelación.

Al establecer y pedir una auditoria con ISO 27000 se puede tomar en consideración que al solicitar son certificados acreditados a las empresas que tuenen auditar y optimización de TIC´S(Herrera Zurita & Duran Cals, 2016)

- OEA
- ISO 9004
- SICTED

- ISO 9001
- UNE EN 13816
- UNE 187001
- ISO 14001
- EMAS: Eco Management and Audit Scheme
- ISO 27001

Después de determinar el riesgo se establece las estrategias de riesgo se determinan mediante el análisis de los riegos con el fin de poder prevenir o combatir un ataque al que se puede ser expuesto.

Estableciendo un análisis con herramientas de seguridad como COBIT y ISO27000 los cuales nos presenta el uso de buenas prácticas para la seguridad de la información que proporciona las

- Evitar riego

Esta estrategia de tratamiento no es comúnmente desarrollada, aunque si se la toma en consideración para poder establecer ciertos parámetros del riesgo informático refiere a aquella eventualidad que imposibilita el cumplimiento de un objetivo, es decir, todo aquel peligro o daño que puede afectar el funcionamiento directo los resultados esperados de un sistema informático.

Respecto a los riesgos que se tratan de evitar son los considerados como los frecuentes y de los que se determina mayor conocimiento para el usuario, con esto se determina que el usuario puede optar como un método de evitar el riesgo de tal manera que sea evitar la acción o el proceso que puede provocar un ataque.

Riesgos de integridad: abarcan todos los riesgos asociados con la autorización, completitud y exactitud de la entrada, procesamiento y reportes de las aplicaciones utilizadas en una organización. Estos riesgos aplican en cada aspecto de un sistema de soporte de procesamiento de negocio y están presentes en múltiples lugares y momentos en todas las partes de las aplicaciones.

Riesgos de relación: refieren al uso oportuno de la información creada por una aplicación. Estos riesgos se relacionan directamente a la información de toma de decisiones (información y datos correctos de una persona/proceso/sistema correcto en el tiempo preciso permiten tomar decisiones correctas).

Algunos métodos de evitar el riesgo en un ambiente cotidiano son los siguientes:

Tabla 11:

Métodos para evitar riesgos

Riesgo	**Evitar riesgo**
Lluvia, cambio de clima	No salir del área segura donde este.
Incendio en un bosque	No encender fogatas
Robo en un banco	No ir al banco
Accidentes de transito	No viajar, no salir en vehículos
Perdida de vuelos	No comprar pasajes para realizar viajes

Nota: Detalle de métodos para la mitigación de riesgos

- Transferir el riego

La trasferencia del riego es lo que la actualidad utiliza de manera frecuente empresas y compañías las cuales utilizan varias formas de asegurar su información sus datos o la infraestructura con equipos, bienes que estén inmersos en el negocio o en la cotidianidad.

Se determinan a los riesgos con mayor causal como los opinados para adquirir este tipo de garantía o de tratamiento para solventar el riesgo al que puede estar expuesto algunos de ellos se detallan a continuación.

Riesgos de acceso: se enfocan en lo que es el acceso inapropiado a sistemas, datos e información. Estos riesgos suponen tanto los riesgos de segregación inapropiada de trabajo, así como los riesgos asociados con la integridad de la información de sistemas de bases de datos y los riesgos asociados a la confidencialidad de esa información.

Riesgos de utilidad: se centran en tres diferentes niveles de riesgo:

- Los riesgos pueden ser enfrentados por el direccionamiento de sistemas antes de que los problemas ocurran.
- Técnicas de recuperación/restauración usadas para minimizar la ruptura de los sistemas.
- Backups y planes de contingencia controlan desastres en el procesamiento de la información.

Riesgos de infraestructura: ocurren cuando en las organizaciones no existe una estructura de información tecnológica efectiva (hardware, software, redes, personas y procesos) para soportar adecuadamente las necesidades futuras y presentes de los negocios con un costo eficiente. Estos riesgos están asociados con los procesos de la información tecnológica que definen, desarrollan, mantienen y operan un entorno de procesamiento de información y las aplicaciones asociadas (servicio al cliente o usuaria/o, pago de aranceles, etc.)

Algunos métodos de transferir el riesgo en un ambiente cotidiano son los siguientes hay que resaltar que son riesgos de alto impacto y media probabilidad:

Tabla 12:

Métodos de transferir el riesgo

Riesgo	**Transferencia**
Robo de bienes casas o vehículos	Aseguradoras.
Perdida o hurto de dinero de entidades bancarias	Bancos internacionales asegurados con pólizas
Incautación de bases de datos	Seguros de hackers los que proporcionan una póliza para recuperar lo perdido.

Nota: Detalle de transferir métodos para la mitigación de riesgos

- Mitigar el riesgo

Es disminuir el impacto o la probabilidad, una buena gestión del riesgo ayuda a mitigar errores y a garantizar la estabilidad de las compañías en los rendimientos financieros. Además, las organizaciones cuentan con una guía que define los procesos y métodos que debe seguir para gestionar el riesgo de forma estructurada y sistematizada.

Aunque en Latinoamérica no hay una cifra oficial de cuántas empresas implementan modelos de gestión del riesgo operacional, se sabe que son pocas las que invierten tiempo y recursos en estas estrategias. De hecho, muchas organizaciones se preocupan sólo por cumplirle a entidades regulatorias, como la Super intendencia Financiera, pero no tienen en cuenta que más allá de cumplir con una norma, una buena gestión ayuda a la efectividad de los procesos.

Otras organizaciones creen que implementar una buena gestión de riesgos es costoso y no incorporan medidas en su día a día y, peor aún, no las ven necesarias porque toda la vida han operado así y “no les ha pasado nada”. Esto sucede, pese a los escándalos por descalabros de compañías emblemáticas por malos manejos en el riesgo operacional.

A lo que se suma, que cuando las empresas implementan un departamento de Gestión del Riesgo, el gerente se desentiende, se le olvida que el éxito de la estrategia es que se involucre directamente en el tema y priorice el manejo de riesgo.

Precisamente, el gerente debe comprender todos los riesgos a los que está expuesta la compañía para establecer los métodos utilizados para equilibrarlos y mitigarlos.

Esa responsabilidad no se le puede delegar a un solo equipo, por el contrario, hay que involucrar a todas las áreas. La gestión del riesgo hay que trabajarla como cultura, porque va transversal a la compañía, hay que tener una metodología única para que todos la entiendan.

- Mitigar la probabilidad:

Determinar procesos para que reduzca la probabilidad con el fin de terminar que el riesgo disminuya.

- Mitigar el impacto:

Determinar procesos para que reduzca el impacto con el fin de terminar que el riesgo disminuya.

Método de mitigar el riesgo en un ambiente cotidiano son los siguientes hay que resaltar que son riesgos de alto impacto y media probabilidad:

Tabla 13:

Métodos de mitigar riesgos

Riesgo	**Transferencia**
Robo de bienes casas o vehículos	Aseguradoras.
Perdida o hurto de dinero de entidades bancarias	Bancos internacionales asegurados con pólizas
Incautación de bases de datos	Seguros de hackers los que proporcionan una póliza para recuperar lo perdido.

Nota: Detalle de transferir métodos para la mitigación de riesgos

Acciones específicas

Las acciones específicas que determinamos para los riesgos expuestos se analizaron mediante el proceso de la metodología para poder obtener el tratamiento óptimo. Los sistemas de información son conjuntos de recursos interrelacionados (pueden ser medios técnicos, el factor humano y los procesos) que promueve la captura de datos, almacenarlos y convertirlos.

Es responsabilidad de los actores de una empresa, mantener la confidencialidad, integridad y disponibilidad de la información, ya que estos procesos son importantes para la organización de la entidad. La seguridad de la información es una prioridad en esta era digital. Así mismo, es relevante concienciar a los involucrados en el uso correcto de este sistema integral, para lo cual se debe afianzar el conocimiento en los siguientes aspectos:

- Entender los tipos de riesgos de seguridad de los recursos informáticos y su implicación en el desempeño del centro.
- Lineamientos para realizar los respaldos de información.
- Buenas prácticas en el manejo y conservación de los soportes informáticos (dispositivos USB, discos compactos, DVD, documentación física, archivos, etc.)
- Buen manejo del correo electrónico.

Principios de comportamiento ético profesional que guíen a los empleados en sus decisiones en el manejo y utilización de los recursos informáticos.

Este proceso lo podemos determinar en algunos aspectos:

Tabla 14:

Descripción de riesgos analizados con respecto con el tratamiento

	RIESGO	TRATAMIENTO
3	Al realiza una suplantación de identidad los riesgos son varios ya que pueden ser legales o llevar a casos extremos como perder la vida ya que hay intereses fuertes cuando asumen estos riesgos.	MITIGAR LA PROBABILIDAD Y EL IMPACTO
4	La suplantación de identidad también es un método de salvaguardar la integridad de una persona ya que en casos legales donde se necesita testigos protegidos se suplanta o simplemente se oculta la identidad de estas personas.	EVITAR EL RIESGO
5	Se lleva a cado el control de base de datos mediante la vulnerabilidad de contraseñas comunes o al no tener conocimiento de buenas prácticas al determinar una contraseña que se proteja	TRANSFERENCIA DEL RIESGO
6	La ingeniería social es una de las vulnerabilidades que provocan uno de los mayores riesgos ya que mediante el análisis de las victimas llevan a cabo el analizar e investigar sus aspectos relevantes para el ataque.	MITIGAR EL IMPACTO
11	Páginas web son las utilizadas para la propagación de virus ya que muchas veces son vinculadas a páginas externas que al abrir la página requerida se abren automáticamente y de esta manera infectan al equipo con virus	EVITAR EL RIESGO
12	Equipos dañados por contaminación ambiental siendo esto un caso de riesgo de manera directa ya que el equipo dejaría de funcionar.	EVITAR EL RIESGO
13	Los equipos sometidos a la humedad muchas veces corren el riesgo de no tener reparación por lo cual se debería realizar la adquisición de un nuevo equipo siendo un casto alto para la empresa.	MITIGAR LA PROBABILIDAD Y EL IMPACTO

Nota: Detalle de riesgos analizados con respecto con el tratamiento para la mitigación de riesgos

Descripción de las acciones específicas

Para determinar las acciones específicas por cada riesgo se desminará a continuación el riesgo el método de tratamiento y las acciones que se pueden tomar.

Tabla 15:

Tratamiento de los riesgos con referencia al mapa de riesgo

	RIESGO	TRATAMIENTO
3	Al realiza una suplantación de identidad los riesgos son varios ya que pueden ser legales o llevar a casos extremos como perder la vida ya que hay intereses fuertes cuando asumen estos riesgos.	MITIGAR LA PROBABILIDAD Y EL IMPACTO
4	La suplantación de identidad también es un método de salvaguardar la integridad de una persona ya que en casos legales donde se necesita testigos protegidos se suplanta o simplemente se oculta la identidad de estas personas.	EVITAR EL RIESGO
5	Se lleva a cado el control de base de datos mediante la vulnerabilidad de contraseñas comunes o al no tener conocimiento de buenas prácticas al determinar una contraseña que se proteja	TRANSFERENCIA DEL RIESGO
6	La ingeniería social es una de las vulnerabilidades que provocan uno de los mayores riesgos ya que mediante el análisis de las victimas llevan a cabo el analizar e investigar sus aspectos relevantes para el ataque.	MITIGAR EL IMPACTO
11	Páginas web son las utilizadas para la propagación de virus ya que muchas veces son vinculadas a páginas externas que al abrir la página requerida se abren automáticamente y de esta manera infectan al equipo con virus	EVITAR EL RIESGO
12	Equipos dañados por contaminación ambiental siendo esto un caso de riesgo de manera directa ya que el equipo dejaría de funcionar.	EVITAR EL RIESGO
13	Los equipos sometidos a la humedad muchas veces corren el riesgo de no tener reparación por lo cual se debería realizar la adquisición de un nuevo equipo siendo un casto alto para la empresa.	MITIGAR LA PROBABILIDAD Y EL IMPACTO

Nota: Detalle de riesgos analizados con respecto con el tratamiento para la mitigación de riesgos

- *Al realiza una suplantación de identidad los riesgos son varios ya que pueden ser legales o llevar a casos extremos como perder la vida ya que hay intereses fuertes cuando asumen estos riesgos.*
    - Mitigar la probabilidad y el impacto

Para reducir la probabilidad debemos realizar una indagación exhaustiva de los datos y así determinar los datos fraudulentos que pueden tener los datos involucraos en la suplantación de identidad. Reducción del impacto el riesgo expuesto no tendría e mismo impacto social si se altera la probabilidad proporciona legalidad en los datos y de esta manera veracidad de los mismos.

- *La suplantación de identidad también es un método de salvaguardar la integridad de una persona ya que en casos legales donde se necesita testigos protegidos se suplanta o simplemente se oculta la identidad de estas personas.*
    - Evitar el riesgo

El evitar el riesgo es poner en efecto el no realizar el hecho es en lo que se enfocan la salvaguardias en cuidar la integridad de algunos testigos protegidos esto de hecho toma el evitar el riesgo e tal manera que pueda ser evitado el riesgo.

- *Se lleva a cabo el control de base de datos mediante la vulnerabilidad de contraseñas comunes o al no tener conocimiento de buenas prácticas al determinar una contraseña que se proteja*
    - Transferencia del riesgo

Para el control de base de datos se puede contratar un seguro que permita realizar soportes y copias de seguridad de las mismas donde también son empresas que prestan capacitaciones de seguridad basándose en normas que puedan aplicarse en la empresa u organización.

- *La ingeniería social es una de las vulnerabilidades que provocan uno de los mayores riesgos ya que mediante el análisis de las victimas llevan a cabo el analizar e investigar sus aspectos relevantes para el atague.*
    - Mitigar el impacto

La mitigación del impacto en el riesgo está dado por en las empresas proteger contra redes sociales e incluso tener un control de aplicaciones de comunicación por intranet o local ya que mientras se encuentre en un ordenador puede producir una inseguridad si no se mantiene procesos que reduzcan el impacto para evitar los ataques o filtración de información.

- *Páginas web son las utilizadas para la propagación de virus ya que muchas veces son vinculadas a páginas externas que al abrir la página requerida se abren automáticamente y de esta manera infectan al equipo con virus*
    - Evitar el riesgo

Lo referente a la navegación para evitar el riesgo que es no utilizar existen herramientas que bloquean el acceso de esta manera podemos terminar que las restricciones son preventivas haciendo que el riesgo no se dé por esta causa.

- *Equipos dañados por contaminación ambiental siendo esto un caso de riesgo de manera directa ya que el equipo dejaría de funcionar.*
    - Evitar el riesgo

Este riesgo se lo puede evitar de una forma concreta o no obteniendo equipos aunque esto truncaría el desarrollo de la empresa u organización otra forma de evitar el riesgo es manteniendo los equipos en los lugares apropiados y evitando riesgos cotidianos ambientales.

- *Los equipos sometidos a la humedad muchas veces corren el riesgo de no tener reparación por lo cual se debería realizar la adquisición de un nuevo equipo siendo un casto alto para la empresa.*
    - Mitigar la probabilidad y el impacto

Para reducir la probabilidad debemos realizar un cuidado solventando con personal profesional dedicado al soporte y cuidado de equipos para que la probabilidad de estos riesgos disminuya

Reducción del impacto el riesgo expuesto no tendría e mismo impacto empresarias si se altera la probabilidad el impacto en los equipos disminuye evitando que la empresa deba adquirir nuevos equipos determinando como perdida para la empresa cuando es caso de daño.

Uso ético de OSINT

Al igual que sucede con la búsqueda de información en Internet, no es conveniente salir a recoger datos sin haber diseñado una estrategia previa, o cuando menos, sin haber reflexionado con detenimiento qué queremos, para qué lo queremos y dónde lo vamos a buscar. Estos pilares son imprescindibles incluso para el caso de la monitorización o vigilancia dela Red, donde a pesar de que no buscamos nada en concreto, sí debemos diseñar planes que incluyan sistemas de alertas tempranas que puedan ser útiles a nuestros intereses. Si bien es cierto que muchas veces no tenemos claros todos los objetivos, podemos realizar un acercamiento inicial que permita una "tormenta de ideas creativa" para diseñar, a continuación, una lista de objetivos finales junto a una estrategia que nos ayude a alcanzarlos.

Algunos de los objetivos de búsqueda de información en Redes Sociales pueden ser los siguientes:

- Contactar o conocer expertos en una materia.
- Vigilar los movimientos de grupos que atentan contra la seguridad, siempre con las consideraciones legales y éticas exigibles.
- Conocer e interactuar con perfiles de influencia.
- Descubrir qué se está haciendo en otros lugares.
- Determinar posibles relaciones entre perfiles y grupos.

Respecto a los objetos de la búsqueda, pueden ser nombres de organizaciones y personas, número de seguidores y a quién siguen, quién está hablando de qué, noticiasen medios de comunicación, etc. El éxito de que el objeto de búsqueda conduzca hacia el objetivo dependerá, además, de la pericia del investigador a la hora de pensar en cuáles son las claves que le facilitarán extraer la información.

Los principales factores para el uso ético de OSINT son:

En el caso del usuario o consumidor, este brinda pequeñas fracciones de información delicada ya sea por el simple uso de una tarjeta de crédito con la cual a la larga se puede inferir sus hábitos de compra, o al llenar una encuesta en línea uno revela datos personales los cuales el usuario espera que la empresa cuide de manera correcta.

- Integridad: La información cuenta con integridad cuando está completa y sin corromper. Esta característica se ve amenazada cuando la información está expuesta a corrupción, daño, destrucción o cualquier otra 9 alteración de su originalidad. La corrupción de la información puede suceder mientras esta almacenada así como durante su transmisión. Muchos virus están diseñados específicamente para dañar la integridad de la información, es por esto que un método para evitar este tipo de ataques es el buscar cambios en la integridad del archivo como por ejemplo en su tamaño (Alepis & Nita, 2018)
- Disponibilidad: La disponibilidad de la información se refiere a la capacidad de acceder a nuestra información cuando lo necesitemos (Perera, 2012). Esta característica nos permite recibir nuestra información si ninguna obstrucción y en el formato deseado.

  La pérdida de disponibilidad puede suceder por algunos factores, entre los cuales tenemos: perdida de energía, fallos en el sistema operativo o en aplicaciones, fallos en la red, entre otros. Cuando se pierde la disponibilidad por un factor externo, como es el caso de un hacker, se refiere comúnmente a este problema como un ataque de denegación de servicios.

Procesos éticos con OSINT

- El hacker ético.

Es llamado hacker la persona con los conocimientos técnicos y las herramientas necesarias para acceder a una red o equipo aprovechándose de una vulnerabilidad en la seguridad del mismo.

El termino hacker siempre fue relacionado con conductas ilegales por lo cual se crea este termino con el fin de definir a la persona encargada de realizar un análisis de la seguridad de un sistema informático y reportar los fallos encontrados en el sistema. A pesar de esto, el hacker debe actuar como un cracker, es decir, deberá realizar las pruebas de intrusión de la misma manera que lo haría una persona con intenciones maliciosas, siendo justamente ahí donde reside la diferencia entre ambos: el hacker ético cuenta con el permiso de aprovechar las vulnerabilidades encontradas, ganar acceso a la red y reportar a las personas responsables sus conclusiones y recomendaciones.

En el caso del cracker este busca aprovecharse de estas vulnerabilidades de manera ilegal, sin ningún permiso, y de esta manera cumplir sus objetivos maliciosos, ya sea el robo de información delicada, modificación de la misma, entre otros(Perera, 2012).

- Hacking Ético

Este enunciado es de suma importancia para la presente investigación ya que las pruebas a realizar en la empresa seleccionada para el estudio, al igual que en un escenario real, serán de carácter ético y sin deseos de causar ningún daño o intrusión a la empresa. Para empezar es importante destacar como los ataques informáticos en la actualidad están afectando a grandes empresas así como a apeguemos negocios. Según datos en un artículo publicado por Los Angeles Times(2015), las pérdidas ascienden por lo menos a una cifra de $375 billones anuales durante el año 2014.

Rathore (2015) define al hacking ético como “la práctica de irrumpir en computadoras sin una intensión maliciosa, simplemente con el fin de detectar amenazas a la seguridad y reportarlas a las personas responsables.”

El hacker ético es el responsable de llevar a cabo esta irrupción usando su conocimiento y herramientas para propósitos defensivos y constructivos.

- Networking en el hacking ético.

Los conocimientos sobre networking son de suma importancia en el hacking ético. Comprender estos conceptos será de muchísima ayuda para el auditor ya que no solo necesita conocer sobre los sistemas que se usan sino también estar muy preparado con respecto a conceptos de esta rama como son switching y routing.

Comprender el stack de protocolos TCP/IP, asi como los correctos conceptos en materias de direcciones IP, servidores y clientes DHCP, VPNs, e interfaces Wi-Fi, permitirán al auditor tener un conocimiento completo para poder llevar a cabo una auditoria de forma eficaz.

Capítulo V

Conclusiones y recomendaciones

Conclusiones

- Se concluye que al analizar las técnicas y métodos de OSINT se evidencio características y parámetros para determinar la situación actual del riesgo determinando las amenazas y vulnerabilidades de seguridad informática que se determina en varios ámbitos en la cotidianidad.
- Los estándares internacionales como COBIT e ISO 27000 establecen procesos pertinentes al estudio, que son requeridos para la seguridad de los sistemas de información, con estos parámetros se determina que la metodología de análisis de riesgo especialmente Octave, usada para el análisis, que tienen una descripción detallada y también aplicaciones informáticas que permiten emplearlas en casos de análisis de gran volumen.
- Se ha diseñado una propuesta metodológica para el empleo ético de los métodos y técnicas de OSINT, tanto en ciberseguridad como en ciberdefensa, para de esta manera aportar a las necesidades administrativas de las empresas, brindando otras posibilidades de uso de OSINT, sin dejar de lado el aporte a la seguridad de la información, para evitar delitos informáticos.
- Se determinó que las técnicas de OSINT consiguen una práctica avanzada del uso de la información que se encuentra disponible libremente en la web contando con el proceso de la metodología analizada las cuales tienen como sus procesos principales la identificación, valoración y tratamiento.
- Es importante el uso de OSINT ya que puede ser un riesgo o una oportunidad, porque el uso de fuentes abiertas puede brindar facilidades para confirmar información o para

protegerla, de esta manera pueden ser utilizados con fines delictivos pero también para búsqueda de información en procesos administrativos o judiciales.

Recomendaciones

- En todo proceso relacionado con la seguridad, se recomienda realizar el análisis de riesgo para orientar el esfuerzo de protección de manera eficiente y eficaz.
- Se recomienda el uso de estándares en cada análisis y para su selección establecer parámetros comparativos que le lleven a la decisión más adecuada de acuerdo al contexto en que se desarrollará el análisis.
- Se recomienda el proceso metodológico para el empleo ético de los métodos y técnicas de OSINT, tanto en ciberseguridad como en ciberdefensa, debería ser promovido para que el objetivo de este trabajo tenga aplicación útil en la protección de la información y minimizar el riesgo de los delitos informáticos.
- Es importante tener un entrenamiento permanente, para conseguir habilidad en el empleo de las técnicas presentadas.
- Aplicar las técnicas y métodos de OSINT considerándolas como riesgo y como oportunidad de conseguir información, usar fuentes abiertas pero con políticas de seguridad adecuadas pero también para búsqueda de información en procesos administrativos o judiciales.

Bibliografía

Akaichi, J. (2014). Cloud computing location-based services for quality health care services delivery. In *Cloud Computing Applications for Quality Health Care Delivery* (pp. 171–185). https://doi.org/10.4018/978-1-4666-6118-9.ch009

Akaichi, J. (2016). Cloud Computing Location-Based Services for Quality Health Care Services Delivery. In *Geospatial Research*. https://doi.org/10.4018/978-1-4666-9845-1.ch035

Alepis, E., & Nita, S. (2018). Mobile application providing accessible routes for people with mobility impairments. *2017 8th International Conference on Information, Intelligence, Systems and Applications, IISA 2017*, *2018-January*. https://doi.org/10.1109/IISA.2017.8316439

Amaya Balaguera, Y. D. (2015). Metodologías ágiles en el desarrollo de aplicaciones para dispositivos móviles. Estado actual. *Revista de Tecnología*, *12*(2). https://doi.org/10.18270/rt.v12i2.1291

Bernard, R., Bowsher, G., Milner, C., Boyle, P., Patel, P., & Sullivan, R. (2018). Intelligence and global health: assessing the role of open source and social media intelligence analysis in infectious disease outbreaks. *Journal of Public Health (Germany)*, *26*(5). https://doi.org/10.1007/s10389-018-0899-3

Bhattacharya, S., Kumar, A., Kaushal, V., & Singh, A. (2018). Applications of m-Health and e-Health in Public Health Sector: The Challenges and Opportunities. *International Journal of Medicine and Public Health*, *8*(2). https://doi.org/10.5530/ijmedph.2018.2.12

Gómez, R., Pérez, D. H., Donoso, Y., & Herrera, A. (2010a). Metodología y gobierno de la gestión de riesgos de tecnologías de la información. *Revista de Ingeniería*, *0*(31). https://doi.org/10.16924/riua.v0i31.217

Gómez, R., Pérez, D. H., Donoso, Y., & Herrera, A. (2010b). Metodología y gobierno de la gestión de riesgos de tecnologías de la información. *Revista de Ingeniería*, *0*(31), 109. https://doi.org/10.16924/riua.v0i31.217

Herrera Zurita, A., & Duran Cals, J. (2016). Aprendizaje automático para la detección de ataques informáticos. *TFG En Enginyeria Informática, Escola D'enginyeria (EE), Universitat Autónoma De Barcelona (UAB)*, *Junio*.

Peddi, S. V. B., Yassine, A., & Shirmohammadi, S. (2015). Cloud based virtualization for a calorie measurement e-health mobile application. *2015 IEEE International Conference on Multimedia and Expo Workshops, ICMEW 2015*. https://doi.org/10.1109/ICMEW.2015.7169853

Perera, C. (2012). The Evolution of E-Health – Mobile Technology and mHealth. *Journal of Mobile Technology in Medicine*, *1*(1). https://doi.org/10.7309/jmtm.1

Rahman, M. N., & Esmailpour, A. (2016). A Hybrid Data Center Architecture for Big Data. *Big Data*

Research, *3*. https://doi.org/10.1016/j.bdr.2016.02.001

Senekal, B., & Kotzé, E. (2019). Open source intelligence (OSINT) for conflict monitoring in contemporary South Africa: Challenges and opportunities in a big data context. *African Security Review*, *28*(1). https://doi.org/10.1080/10246029.2019.1644357