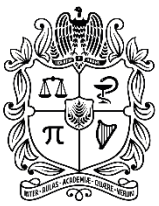


UNIVERSIDAD
NACIONAL
DE COLOMBIA

Marco de Gestión de Riesgos de Tecnologías de Información y Comunicación en un entorno multi empresarial, basado en análisis de datos de seguridad (logs) para la empresa CasaLuker S.A

Jorge Andrés Ramírez Granada

Universidad Nacional de Colombia
Facultad de Administración, Departamento de informatica y Computación
Manizales, Colombia
2021

Marco de Gestión de Riesgos de Tecnologías de Información y Comunicación en un entorno multi empresarial, basado en análisis de datos de seguridad (logs) para la empresa CasaLuker S.A

Jorge Andrés Ramírez Granada

Trabajo final de maestría presentado como requisito parcial para optar al título de:
Magister en Administración de Sistemas Informáticos

Director (a):
PhD. Francisco Javier Valencia Duque

Línea de Investigación:
Riesgos Organizaciones y de Tecnologías de Información

Grupo de Investigación:
Grupo de Investigación en Teoría y Gestión de Tecnologías de la Información

Universidad Nacional de Colombia
Facultad de Administración, Departamento de informática y Computación
Manizales, Colombia
2.021

Dedicatoria

A mis padres, por todo su apoyo, comprensión, actitud y los valores inculcados de sobre salir en los retos académicos y laborales.

A mis amigos muy cercanos considerado como parte de la familia en su gran aporte y apoyo para cumplir las metas propuestas

A Dios por brindarme la paciencia y voluntad para establecer mi rumbo hacia buenos horizontes.

Declaración de obra original

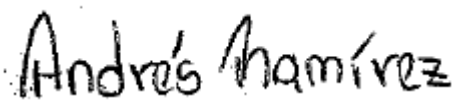
Yo declaro lo siguiente:

He leído el Acuerdo 035 de 2003 del Consejo Académico de la Universidad Nacional. «Reglamento sobre propiedad intelectual» y la Normatividad Nacional relacionada al respeto de los derechos de autor. Esta disertación representa mi trabajo original, excepto donde he reconocido las ideas, las palabras, o materiales de otros autores.

Cuando se han presentado ideas o palabras de otros autores en esta disertación, he realizado su respectivo reconocimiento aplicando correctamente los esquemas de citas y referencias bibliográficas en el estilo requerido.

He obtenido el permiso del autor o editor para incluir cualquier material con derechos de autor (por ejemplo, tablas, figuras, instrumentos de encuesta o grandes porciones de texto).

Por último, he sometido esta disertación a la herramienta de integridad académica, definida por la universidad.



Jorge Andrés Ramírez Granada

Fecha 22/10/2021

Agradecimientos

Mis Agradecimientos son remitidos aquellas personas que intervinieron en mi proceso académico, en mi formación, colaboración y apoyo como los integrantes de la empresa CasaLuker S.A quienes me brindado su espacio, su carisma y buena actitud ante mi proceso educativo y la empresa en general por su aporte en conocimiento y tecnología. Agradecimiento a mi director de trabajo el profesor Francisco Javier Valencia por su interés y apoyo permanente en las asesorías, a la Universidad Nacional de Colombia sede Manizales por la calidad de sus instalaciones y docentes.

Resumen

Marco de Gestión de Riesgos de Tecnologías de Información y Comunicación en un entorno multi empresarial, basado en análisis de datos de seguridad (logs) para la empresa CasaLuker S.A

Las organizaciones corporativas como CasaLuker, objeto del actual estudio, establecen diferentes estrategias de funcionamiento como lo es la aplicación parcial de la misma tecnología para sus operaciones diarias en función del macroproceso, lo cual es la razón de ser de una empresa. Por consiguiente, se requiere de la protección de la información como activo primordial que, por lo regular, es supervisada desde el área “Tecnología de la Información”, quien provee y parametriza herramientas tecnológicas que proporcionan registros (Logs) sobre las amenazas que afectan la seguridad de la información. Por tanto, la gestión del riesgo se convierte en un proceso de vital importancia para mitigar el posible impacto negativo generado por la materialización de un evento que ocasione un daño en los activos de la empresa, con ello se garantiza la continuidad de las operaciones de la empresa. El presente estudio abarca una revisión de la literatura acerca de los marcos metodológicos sobre la gestión del riesgo de Tecnologías de Información y Comunicación. Se elige OWASP Risk Rating por ser un modelo flexible y ligero para establecer y validar una propuesta basada en eventos de amenazas de seguridad de la información mediante los 212.690 registros (Logs) obtenidos de las herramientas tecnológicas existentes del entorno multi empresarial. De esta forma, se presentaron aportes tangibles sobre el estado actual de las amenazas detectadas como parte de los insumos en la toma de decisiones respecto al mejoramiento de la barrera de seguridad de la información.

Palabras clave: (Seguridad de la Información, Metodología, Riesgos, OWASP, Logs, Herramientas Tecnológicas)

Abstract

Information and Communication Technology Risk Management Framework in a multi-business environment, based on security data analysis (logs) for the company CasaLuker S.A

Corporate organizations such as CasaLuker, object of the current study, stablish different operating strategies such as the partial application of the same technology for their daily operations based on their macro process, which is the reason for being of a company. Therefore, the protection of information is required as a primary asset, usually supervised from the "Information Technology" area, which provides and parameterizes technological tools that provide records (Logs) on the threats affecting information security. Therefore, risk management becomes a process of vital importance to mitigate the possible negative impact generated by the materialization of an event that causes damage to the company's assets, thereby guaranteeing the continuity of the operations of the company.

This study includes a review of the literature on the methodological frameworks on the risk management of Information and Communication Technologies. OWASP Risk Rating was chosen for being a flexible and lightweight model to establish and validate a proposal based on information security threat events through the 212,690 records (Logs) obtained from the existing technological tools of the multi-business environment. In this way, tangible information is provided on the current status of the threats detected as part of the inputs in decision-making regarding the improvement of the information security barrier.

Keywords: (Information Security, Methodology, Risks, OWASP, Logs, Technological Tools)

Contenido

Lista de Ilustraciones

Pág.

Lista de tablas

Pág.

Introducción

La seguridad de la información es un elemento que ha trascendido en la evolución de las necesidades corporativas puesto que se volvió un activo de gran importancia, ya que en ella radican estrategias pasadas, presentes y futuras en el desarrollo del modelo productivo. Es así, que las organizaciones han ido estableciendo medidas para garantizar la protección de la información, al percibir que esto es una necesidad y requieren implementar medidas para garantizar la continuidad del negocio. Las exigencias del mundo comercial demanda estar a la vanguardia de certificaciones o auditorias para soportar las operaciones que la empresa actualmente este realizando o a su vez prometedoras inversiones para nuevos proyectos, si quiere ser reconocida como un ente competitivo para aplicar a diferentes aspiraciones de crecimiento.

Ahora, es allí donde radica una gestión sobre los riesgos enfocada a la seguridad de la información según las necesidades corporativas para visualizar una panorámica de lo que la empresa puede tolerar al presentarse un evento adverso, en cualquiera de sus dependencias o procesos catalogados como críticos y que por lo regular están enfocados hacia la confiabilidad, integridad y disponibilidad de la información. La gestión del riesgo se convierte en un análisis de todos los factores que pueden acontecer y de allí, se establecen los escenarios de riesgos para calcular una probabilidad de ocurrencia e impacto que este puede generar y con el cual se pueda establecer una severidad del riesgo que da origen al establecimiento de controles y planes de mejoramiento. Lo anteriormente mencionado se basa en un estándar de las diferentes metodologías de riesgos existentes, como las referenciadas en el presente documento en el que se describen de forma general su forma de ejercer el proceso. A partir de esto, se selecciona la metodología OWASP Risk Rating como un modelo ligero, fácil de implementar y enfocado hacia la seguridad de la información y al cual se plantea una propuesta basada en las herramientas tecnológicas existentes en una empresa como CasaLuker S.A, quien actúa bajo un entorno multi empresarial donde varias empresas dependen de la misma área de Tecnología de la Información.

Las herramientas tecnológicas invertidas por parte de la organización son elementos que muchas veces no son tenidos en cuenta, no muestra más de su importancia a parte de cumplir su objetivo principal de funcionamiento. Pero estas herramientas traen suministros adicionales como registros (Logs) que son guardados periódicamente que con una valoración adecuada se puede extraer de allí comportamientos que permitan tomar acciones preventivas y correctivas en el buen hacer de los procesos vigentes.

El presente estudio establece un criterio de referencia, el cual consiste en tomar esos registros (Logs) como parte de un insumo para adaptarlo a una metodología de riesgos como lo es OWASP. A partir de allí se recolectan los eventos de ocurrencias en amenazas detectadas de las empresas que conforman ese entorno multi empresarial que de forma cuantitativa permiten calificar de una forma más objetiva algunos de los criterios definidos por la metodología OWASP y los demás quedan a juicio cualitativo que de cierta forma pueden definir posturas con la evidencia recolectada.

Por tanto, las evidencias recolectas contribuyen a la evaluación realizada para el cálculo de la severidad del riesgo y a partir de ello, estimar los controles necesarios para la mitigación bajo una propuesta de que arreglar que consiste en un plan de tratamiento. Adicional, se ilustra todo lo que las herramientas han podido capturar justificando la inversión hecha por la compañía para plasmar nuevos escenarios en la renovación tecnológica ante los nuevos eventos en vulnerabilidades y amenazas al igual que el cumplimiento de las exigencias del mercado.

Capítulo 1. Propuesta de investigación

1.1 Situación encontrada

El entorno organizacional actual concibe las Tecnologías de Información y Comunicación como un recurso vital para los negocios y como tal requiere de una adecuada protección. La infraestructura tecnológica que poseen las organizaciones debe ser oportunamente protegidas para garantizar el cumplimiento de sus objetivos y es allí donde surge la dependencia de la gestión de riesgos, concebida como una serie de procesos que adecuadamente implementados permiten disminuir la incertidumbre. De tal forma que, una buena gestión de riesgos permite afianzar la información en términos de disponibilidad, confidencialidad e integridad (ENISA, 2006).

A pesar de todas las recomendaciones divulgadas por diferentes medios, los integrantes de las organizaciones no siempre comprenden la necesidad de un modelo de seguridad basado en los riesgos, quizás por un desconocimiento al no tener eventos registrados que realmente le hubiesen afectado y mucho menos si se cuenta con presupuestos reducidos para inversiones tecnológicas. Un factor adicional, son las alianzas empresariales dependen de la misma área como ente responsable de protección (Tecnología de la Información - TI) donde suponen realizan las protecciones adecuadas sin que esta se guie aun estándar. Como se expresa en el documento CONPES de Seguridad Digital, se observa la necesidad de educar y promover una cultura de conciencia en la que el riesgo es la responsabilidad de cada integrante del entorno al que pertenezca y discrimina la gestión del riesgo como uno de los elementos más importantes de la seguridad (CONPES, 2016), ya que permite el entendimiento de los procesos de la compañía y las amenazas a

las que está expuesta con el propósito de generar las acciones que mitiguen, eliminen o controlen los efectos negativos que pudiesen dar (ISO/IEC, 2009).

Por otro lado, el Departamento de Tecnología de la Información puede tener herramientas que sirven de protección de seguridad hacia los diferentes sistemas de las empresas que soportan y estos a su vez generan datos como es el caso de los Logs, pero mucha de la información que allí se registra no es analizada ni estructurada por diversos factores, la cual serviría como un complemento para un marco de gestión de riesgos.

La empresa para construir el modelo es una organización local de la ciudad de Manizales del departamento de Caldas, llamada CasaLuker S.A. La empresa maneja un entorno asociado con varias empresas (Alianza estratégica) en diferentes definiciones de negocios (Multi empresarial) bajo la misma infraestructura tecnológica, tiene herramientas que permiten gestionar las incidencias relacionadas con la seguridad que pueden contribuir a la construcción de un Marco de Gestión de Riesgos en Tecnología de la Información y Comunicación.

Las diferentes metodologías de gestión de riesgos tanto organizacionales como tecnológicas adolecen por lo general de un adecuado soporte estadístico para evaluar el efecto del riesgo, orientar las prácticas y supervisar los objetivos con las métricas respectivas hacia los problemas que se puedan identificar (Valencia et al., 2016a). Considerando lo anterior y aprovechando el uso de herramientas implementadas en las organizaciones, el modelo se fijaría en datos y hechos tangibles y no en estimaciones, permitiendo cerrar brechas de seguridad de las potenciales amenazas a que están expuestos los activos tecnológicos y ello es una de las principales preocupaciones de la comunidad empresarial y en particular de CasaLuker.

La adecuada y pertinente identificación de riesgos en el contexto del negocio requiere no solo de la experticia de los responsables de los procesos y de las tecnologías de la organización, sino contar hasta donde sea posible con estadísticas que respalden la identificación de cualquier tipo de amenaza en la organización para poder realizar una adecuada gestión de ella. Una amenaza se define como un evento negativo que podría

causar diferentes incidentes en las empresas, generando daños en sus sistemas o perdidas en sus activos como por ejemplo la información (Amutio Gómez, 2012). Microsoft, en una encuesta de percepción muestra las principales preocupaciones en las organizaciones, donde los riesgos cibernéticos superan a otros por un buen margen (Marsh, 2019). La XIX encuesta nacional de seguridad informática 2.019 soportada por la Asociación Colombiana de Ingenieros de Sistemas (ACIS) no está lejos de otros resultados, puesto que indica que el 55% de los incidentes de seguridad están categorizados en riesgos de ciberseguridad (Almanza J., 2019).

Para el caso específico de CasaLuker y sus filiales, se han venido almacenando una serie de logs de incidentes en las plataformas tecnológicas, a través de herramientas como portal administrativo de office 365, Consola de firewall FortiGate (Seguridad Perimetral), Consola de administración de antivirus Sophos entre otros, sin que hasta el momento sean analizadas como parte de una estrategia de control y gestión análisis de riesgos. Las tendencias internacionales muestran la necesidad de aportar valor a las organizaciones, extendiendo la visión de seguridad como una fuente que complemente su sistema hacia los objetivos del negocio (Marsh, 2019).

La investigación dentro de este entorno permitirá modelar un sistema de gestión de riesgos, considerando el análisis de datos con las herramientas existentes, eventos catalogados como críticos y las metodologías actuales dentro de un marco multi empresarial teniendo en cuenta la evolución de la tecnología. En este sentido la propuesta tiene un valor preventivo, respaldado con hechos y datos reales del día a día en la ejecución de las operaciones de las compañías. De tal forma que, es más sencillo apalancar posturas de seguridad de la información que apunten a los objetivos del Core de cada negocio.

1.2 Justificación

La importancia de la seguridad de la información es un factor que al pasar de los tiempos se ha convertido en la conciencia empresarial de valorar y proteger todos los activos de

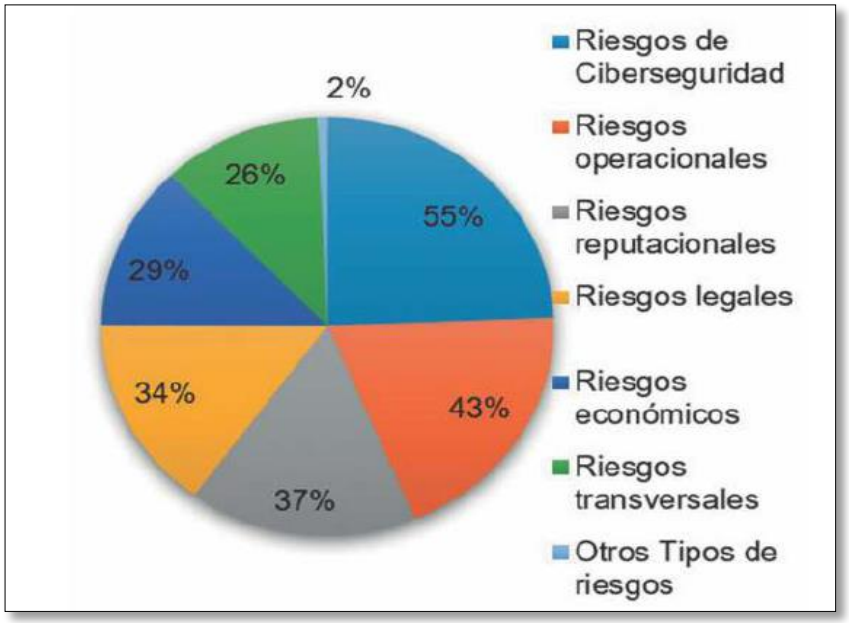
información ante las diversas amenazas a las que se encuentran expuestas. La seguridad de la información es una necesidad, MINTIC define este término con base en (ISO/IEC 27000), como la preservación de la disponibilidad, integridad y confiabilidad de la información (MinTIC, 2015), todo esto con énfasis en asegurar la operación de los diferentes procesos que posee una compañía, que va de la mano con una buena gestión de riesgos de las tecnologías de la Información y comunicación.

Más complejo se vuelve el escenario de un marco de seguridad, cuando la administración de esta es soportada por el área de Tecnología de la Información en un contexto multi empresarial, donde implica trabajar bajo la misma infraestructura de red, políticas, ubicación geográfica y diferentes condiciones de los negocios, para el desarrollo del Core de negocio bajo sus estrategias comerciales y corporativas. Es por ello, que se determina la necesidad de estructurar un modelo de gestión de riesgos en tecnologías de la Información y Comunicación, donde se identifiquen el impacto y efecto que pueden generar las vulnerabilidades mediante el análisis de datos (Logs) sobre dispositivos o consolas dispuestas por el área de Tecnologia de Información, datos tangibles que aportan comportamientos o tendencias de los eventos, lo cual con una metodología por sí sola no se aprovecharía, puesto que estas en la mayoría se basan de percepciones que se podrían volver subjetivas de lo que pudiese ocurrir. Por tanto, las empresas podrían mitigar los eventos de riesgos, saber que la infraestructura invertida contribuye a que sus organizaciones sean más seguras y apalanquen otros procesos en beneficio de soportar una propuesta antes los líderes de las empresas en temas relacionados con Tecnología de la Información y Comunicación.

La XIX Encuesta Nacional de Seguridad Informática (Almanza J., 2019), indica los motivos por los cuales no se realiza una gestión de riesgos considerando factores como: el bajo presupuesto asignado por las compañías, el no tener un proceso formal de gestión del riesgo dentro de una organización y la falta de conocimiento para la aplicación de una metodología como se expresa en la **Ilustración 1-1**. Adicional, se estipulan los riesgos más representativos evidenciado en la **Ilustración 1-2** en el que el riesgo de ciberseguridad está por encima de los riesgos operacionales.

Ilustración 1-1. Razones para no realizar la Gestión del Riesgo.

Ilustración 1-2: Tipos de Riesgos



Fuente: Tomado de (Almanza J., 2019)

De tal forma que un valor agregado para una empresa es el establecimiento de una buena gestión de riesgos en la seguridad de la información para mantenerse en la dinámica y exigencias de los negocios que requieran de certificaciones nacionales e internacionales, auditorias, confiabilidad de los clientes y competencias comerciales ante sus similares.

Esta investigación aporta a la empresa datos sobre la seguridad de la información, un marco de gestión de riesgos con datos reales de las incidencias o amenazas que se han presentado y la viabilidad de aplicar este en una de las empresas que depende del área de tecnología de Información para mejorar la confiabilidad en sus procesos organizacionales, sin alterar su funcionamiento como resultado final de su actividad comercial. También es un insumo que puede ser replicado en otras empresas del sector que contenga un modelo similar hacia la gestión de la información en términos de seguridad.

1.3 Marco teórico y trabajos relacionados

1.3.1 Seguridad de la Información

La seguridad de la información es un concepto que ha tomado bastante relevancia en las organizaciones, la forma de aplicar está en la ejecución de actividades diarias y que aporte en la disminución de la incertidumbre que ponga en vilo las operaciones de las compañías, su prestigio y estrategias comerciales. La seguridad de la información esta propiamente enlazada con la información y está a su vez es considerada como un activo de gran importancia para las organizaciones (Valencia-Duque & Orozco-Alzate, 2017), puesto que es un insumo para soportar las estrategias de negocio y darle la continuidad en el tiempo. La seguridad de la información según la definición dada por la ISO 27000, indica la preservación de la confiabilidad, disponibilidad e integridad de la información (ISO/IEC 27000, 2018) e identifica otras propiedades como la autenticidad y la responsabilidad.

1.3.2 Gestión del Riesgo

La mayoría de información está vulnerable a las diferentes amenazas del mundo tecnológico como los ciberataques, phishing, accesos no autorizados, fraudes electrónicos, suplantación de identidad entre otros; y la dinámica constante en la evolución de técnicas, tecnologías e instrumentos, que exige a las organizaciones mejorar cada vez más su seguridad, mediante mecanismos como políticas de seguridad, hardware, software y protocolos que, asociados entre sí, sostengan niveles aceptables en el riesgo de la información organizacional. Por tanto, la gestión del riesgo coordina actividades para

controlar una organización ante los eventos, amenazas y las posibles consecuencias que ponga en riesgo el funcionamiento de la compañía (ISO/IEC 27000, 2018).

Un informe de World Economic Forum indica en términos de impacto y probabilidad los diez principales riesgos mundiales donde están referenciados los ataques cibernéticos, fraude y robo de datos (WEF, 2019), muestra la importancia de generar mecanismos que mitiguen las vulnerabilidades de las empresas en la seguridad de la información.

El riesgo en la seguridad de la información, debe ser una parte estratégica de los procesos que dirige una compañía (FERMA, 2003), considerando todos los elementos de una forma metódica, identificando los riesgos en los diferentes activos de la información y la forma de tratarlos, con el propósito de disminuir la incertidumbre (ISO/IEC 27000, 2018).

1.3.3 Metodologías, Marcos y Normas de Gestión de Riesgos

Existen diferentes metodologías de gestión del riesgo en Tecnología de la información y Comunicación que, adaptadas a una buena gestión de los líderes y responsables, contribuyen al bloque defensivo ante los diferentes escenarios que se puedan producir; y a partir de ello establecer medidas según la importancia de lo que los directivos, accionistas o dueños requieran.

Se establecen diferentes criterios de búsqueda para obtener información sobre la Gestión del Riesgo en Tecnología de la información y Comunicación basado en los siguientes términos: Risk Assessment methodology, Information security risk assessment, Risk Assessment methodology comparison, Information Security Management System, ISMS, Information security, framework for comparison, methodologies y information security risk analysis.

El análisis de los riesgos realizados por cada metodología busca tener un panorama de los activos de la organización para identificarlos y priorizarlos según las necesidades

corporativas, esto implica un monitoreo constante sobre las amenazas latentes y la probabilidad de la ocurrencia de alguna de ellas (Zabawi et al., 2015).

Algunas metodologías de Gestion de Riesgo trabajan diferentes criterios que son adecuados a las circunstancias de un modelo negocio para ofrecer un dimensionamiento de las vulnerabilidades y a cuál de estas debe darle la importancia. Desde la parte cuantitativa, Zabawi indica que ISRAM y CORA ofrecen una determinación de las consecuencias sobre los incidentes, permitiendo obtener información de los costos y beneficios sobre las protecciones que se deben utilizar, de tal forma que el modelo sería más preciso puesto que usa herramientas matemáticas para dar una visitón más acertada del riesgo (Zabawi et al., 2015). Sin embargo, indica que en entornos grandes se pudiese complicar la aplicación del modelo según la precisión requerida. Esto podría ser un factor de desventaja que limite su uso en un entorno multi empresarial en la que existen diversos modelos de negocio a lo cual distorsione su ejecución. Este mismo autor menciona que desde la parte cualitativa las metodologías que se resalta son OCTAVE, CORAS y CRAMM, puesto que permite determinar áreas con gran probabilidad de riesgo en un menor tiempo y la lingüística es más sencilla por el uso de adjetivos. En su contra podría estar el análisis que den los involucrados por el manejo de la subjetividad de la importancia que le pudiesen dar en la priorización de riesgos y selección de protecciones (Zabawi et al., 2015).

ISRAM (Information Security Risk Analysis Method), esta metodología se basa en encuestas para determinar el riesgo, la probabilidad y la consecuencia donde intervienen los gerentes y demás personal. Cuantifica un valor cualitativo para alto, medio y bajo. Un comparativo realizado por (Vorster & Labuschagne, 2005) destaca esta metodología pero al igual que OCTAVE necesita de una preparación extensa lo cual no la hace la más rápida para obtener resultados y esto podría ser un factor no muy agradable para los dirigentes pero al gastar más tiempos en sus pasos de preparación puede llegar a ser mucho más exacta que otras metodologías.

CORAS maneja elaboración de modelos usando los expertos del negocio y se basa en un lenguaje grafico como lo es UML (Unified Modelling Language) de tal forma que facilita la comunicación entre las partes del proceso de análisis de riesgos para el tratamiento correspondiente en la identificación de salvaguardas, esto favorece la aplicabilidad (PANDEY, 2012). Según (Bornman & Labuschagne, 2004) no existe un procedimiento para la aceptación de riesgos residuales que se referenciaría como un desventaja. Otro autor indica que se debe ampliar una fase de requisitos puesto que la metodología es muy generalizada y la precisión de esta podría no ser muy asertiva si no se tiene claro la dirección concreta (PANDEY, 2012).

CRAMM (Risk Analysis and Management Method) esta metodología maneja etapas organizadas tomando criterios técnicos y no técnicos en la evaluación de activos, amenazas y vulnerabilidades para aplicar las medidas necesarias manteniendo la gestión activa sobre los riesgos. Una de sus ventajas es la compatibilidad que tiene con la ISO 27001 lo cual afianza sus criterios de análisis en la ejecución del modelo metodológico. Una deficiencia es la evaluación cuantitativa puesto que no la proporciona y su enfoque es direccionado hacia lo cualitativo (PANDEY, 2012).

COBIT (Control Objectives for Information and related Technology), ofrece una metodología muy amplia, robusta y con una generalidad de su forma de gestionar los procesos de una organización, enfocando gran parte hacia la gobernanza. Dentro de sus módulos tiene la gestión del riesgo en la que involucra a las áreas funcionales. Un comparativo realizado por (Susanto et al., 2011) muestra las bondades de esta metodología que se visualiza como un estándar que comparado con la ISO 27001 y la gran experiencia en el manejo de política en la seguridad de información desde el punto de vista de la gobernanza.

(Bornman & Labuschagne, 2004), indica que CRAMM, OCTAVE y CORAS no logran un equilibrio entre los diferentes tipos de controles, les falta una gestión de integración entre estos y requieren un proceso de formalización en la comunicación entre incidente.

La metodología EBIOS se basa en un método de criterios comunes (CC), analizan el contexto, generan las necesidades, estudian las amenazas con las que se enuncian los objetivos para determinar los requerimientos en seguridad que como resultado aporten a la gestión del riesgo por medio de contramedidas y acciones que se deban tomar (Fabisiak et al., 2012). El análisis realizado por este autor indica que EBIOS fue la mejor metodología comparada con Mehari, CRAMM, OCTAVE y COBRA puesto que principalmente se enfoca a la gestión de la seguridad de la información y está disponible de forma gratuita.

OCTAVE es una metodología con varias alternativas según la dimensión de las empresas generando versiones de sí mismas como OCTAVE-S, Allegro y OCTAVETE. Se basa en los conocimientos y experiencias de los colaboradores para construir perfiles de amenazas en el riesgo que se pudiese dar. Como su ventaja principal es la documentación basada en los patrones en los cuales se puede personalizar según la organización. Como desventaja es su complejidad y la limitación del modelamiento cuantitativo (Singh & Joshi, 2018) y podría excluir conceptos como la autenticidad, responsabilidad y auditabilidad para mejorar la evaluación de riesgos (PANDEY, 2012). Una metodología similar a esta es NIST RFM (Instituto Nacional de Estándares y Marco de Gestión de Riesgos Tecnológicos) puesto que seguí conceptos, pero es más usaba como una guía de apoyo que una metodología en sí misma.

Otra metodología es FAIR (Factor Analysis of Information Risk), está apunta hacia las debilidades relacionadas con la seguridad permitiendo normalizar el riesgo mediante la comprensión del tiempo gastado y el dinero invertido hacia la afectación de seguridad que se pudiese dar en una organización.

(Singh & Joshi, 2018) genera un comparativo en la que no define cual sería la mejor metodología, pero ofrece pautas para analizar desde el punto de vista en costo, complejidad, herramientas entre otros en donde OCTAVE pudiese cumplir como apoyo a las organizaciones en su proceso de llevar a cabo la gestión del riesgo y la aplicabilidad de este.

COBRA (Consultative, Objective and Bi-functional Risk Analysis), dentro de sus fortalezas está la automatización de procesos dando crédito a la evaluación de riesgo para que sea más sencillo, posee pasos claros al momento de ejercer una implementación mediante una secuencia de instrucciones donde se aplica una caracterización del sistema, se identifican amenazas al igual que olas vulnerabilidades para estimar los controles e impacto que a su vez determinan el riesgo. Entre los puntos negativos estaría el enfoque hacia la seguridad de la información en términos de integridad, confidencialidad y disponibilidad y la claridad sobre la evaluación de riesgo con base en el autor (PANDEY, 2012)

(PANDEY, 2012) aplica una comparación bajo conceptos de cuantificación, Integración de seguridad en atributos, integración de amenazas y vulnerabilidades, precisión y validación, estándar de conformidad y herramientas en la que se destaca la metodología CRAMM obteniendo mejores calificaciones sobre COBRA, CORAS y OCTAVE.

(Agrawal, 2017) realiza un comparativo en la que enmarca las metodologías CORAS, CIRA, IS como funcionales e ISRAM como comparativa rescatando su simplicidad como lo hizo (Vorster & Labuschagne, 2005). En el nivel experiencia IS requiere de expertos, CORA y CIRA requiere de especialistas o colaboradores que manejen un nivel medio para su funcionamiento mientras que ISRAM es autodirigido donde incluye equipos de la propia organización lo cual indica la facilidad de uso. Si una organización requiere que se base estrictamente en los estándares de Tecnología de la Información CIRA E IS no son la alternativa. Este autor según los resultados indica ISRAM como la opción a considerar puesto que no se requiere de un experto.

Mehari tiene un enfoque hacia la seguridad y usa una serie de pasos como la identificación del riesgo y una serie de evaluaciones como factores disuasivos y preventivos, impacto y la reducción de este, riesgos globales y toma de decisiones si se aplica la aceptación del riesgo entre otros (Syalim et al., 2009), no incluyen un control después del análisis de riesgos.

Magerit es una metodología de análisis y gestión de riesgos de los sistemas de información, involucra activos de importancia para la organización y sobre estos aplica que

costo tendría si tuviese una degradación causado por amenazas para determinar las medidas de salvaguardas para hacerlos efectivos según el impacto que este provoque (Tejena-Macías, 2018). (Syalim et al., 2009) indica que esta metodología no incluye un control después del análisis de riesgos.

La metodología OWASP Risk Rating Methodology clasifica los riesgos bajo una serie de pasos que incluye la identificación, la probabilidad de ocurrencia, el impacto que estos pueden generar para determinar la gravedad del riesgo en la organización y con base en ello estructurar una priorización para obtener la calificación total de los eventos y riesgos a considerar (Owasp, 2013). Está metodología busca la practicidad en la que los expertos de las organizaciones puedan tomar posturas concretas sobre las decisiones, según el resultado de las evaluaciones como parte de la evolución de la tecnología, conocimiento, tendencias del negocio y facilidad en la aplicación de medidas.

OWASP muestra una construcción de elementos basados en la comunidad y las experiencias que han tenido de forma relevante que permite establecer criterios para la debida atención de una organización ante los diferentes riesgos. Estos elementos se definen en 10 términos como: Inyección, Autenticación, exposición de datos sensibles, entidades externas, control de acceso, configuración incorrecta de seguridad, cross-site scripting, deserialización insegura, uso de componentes con vulnerabilidades y registro y/o monitoreo insuficiente (OWASP Top 10-2017, 2003), cada una de estos elementos permite enfocar esfuerzos sobre actividades que mitiguen el riesgo bajo una identificación de diferentes escenarios y a partir de estos se genera el respectivo enfoque de diversas acciones de protección.

Un comparativo realizado por (Wangen et al., 2018) indica que ninguno de las metodologías está totalmente completa en CURF (Core Unified Risk Framework) pero la ISO / IEC 27005: 2011 es la que más se aproxima según la evaluación de criterios dados en los resultados seguido de FAIR en la que indican hay poca disponibilidad de información sobre la cuantificación de probabilidades. La ISO / IEC 27005 maneja un proceso que incluye actividades de entrada y salida de cada tarea, estos están centrados en los activos,

las amenazas a la que se encuentra expuesta una organización, los controles que permitan mitigar esas vulnerabilidades, las consecuencias o efectos y las probabilidades de las ocurrencias. Esta metodología es considerada como una de las que más se usan.

Las diferentes intervenciones realizadas por los autores no concretan sobre la tendencia de una metodología de gestión de riesgos como la mejor, puesto que cada una maneja criterios relevantes. Sin embargo el autor (Wangen et al., 2018) mediante CURF sobresalta la calificación de la ISO / IEC 27005 como un referente metodológico para afianzar los esquemas de seguridad corporativa. No obstante, OWASP ofrece mecanismos ligeros para toma de desiciones oportunas (Schoenfield, 2015) que con los datos recolectados de la herramientas tecnologicas existentes de la empresa (Logs), permitiran dirigir y exponer los riesgos latentes con base en las necesidades dentro del entorno multiempresarial según la actividad de negocio. OWASP permite clasificar el riesgo para problemas relacionados con la seguridad (B. S. et al., 2019), un modelo de facil adaptación que permite comprender los diferentes escenarios de riesgos y como darles un buen manejo.

La actualización más reciente de OWASP aporta hacia los critearios de evaluación de la seguridad de la información con base en las herramientas que se puedan tener en una orgnizacion como lo son los ataques de injección, este consiste en el envio de datos no confiables a una base de datos de tal forma que, el atacante puede acceder a la información sin la autorización oportunda de los administradores o propiertarios de esta. Otro concepto es basado en la autenticación, esta puede ser robada y a partir de allí es considerado como una suplantación de identidad donde el atacante puede obtener mayores beneficios en la captura de datos sensibles llevando esta amenaza a otro nivel que es la exposición de datos confidenciales. Otro riesgo de seguridad es el control de acceso cuando este es comprometido, ya que puede causar un deterioro de la información por alteraración o divulgación de esta. El concepto de un diseño inseguro tambien hace parte del top diez en el que la recomendación es, la consolidación de las amenazas latentes y comportamientos para apalancar la confiabilidad e integridad de la información (OWASP, 2021).

Los autores (Burkert et al., 2022) coinciden que el aporte ofrecido por la metodologia OWASP les permitió mitigar los riesgos de la aplicación que ellos evaluaron, al igual (Flores Urgilés et al., 2018) en su trabajo les facilitó identificar los riesgos más propensos referenciados a la seguridad en el control de acceso y la exposición de datos de tal forma que, les brinda una planeación sobre las acciones que deben considerar y el impacto positivo que este puede tener. OWASP permite establecer metricas de forma periodica, una estandarización que se va perfeccionando antes las vulnerabilidades y ataques en una empresa desde diferentes enfoques (Pinzon G. et al., 2013). Por tanto, el aporte de las herramientas e inversiones tecnologicas que emiten registros (logs) que combinados con el marco metodologico OWASP, permite generar una medición más acertiva para condicionar los planes de mitigación, que tan oportuno son los esquemas actuales y que mejoras se deben aplicar.

Una de los motivos por los cuales se seleccionó OWASP se debe por lo general a que las demas metodologias de gestion de riesgos de tecnologia de informacion no incorporan parametros especificos para determinar la probabilidad y el impacto lo que genera cierto nivel subjetividad al momento de valorar el riesgo.

1.4 Objetivo general

Elaborar un Marco General de Riesgos de Tecnologías de la Información y Comunicación en un entorno multi empresarial, basado en análisis de datos de seguridad (logs) para empresa CasaLuker S.A

1.5 Objetivos específicos

- Identificar las metodologías de Gestión de Riesgos de Tecnologías de la Información y Comunicación con énfasis en ambientes multi empresariales.

- Analizar los datos (logs) de las herramientas tecnológicas del entorno multi empresarial de CasaLuker S.A y filiales en términos de seguridad de la información.

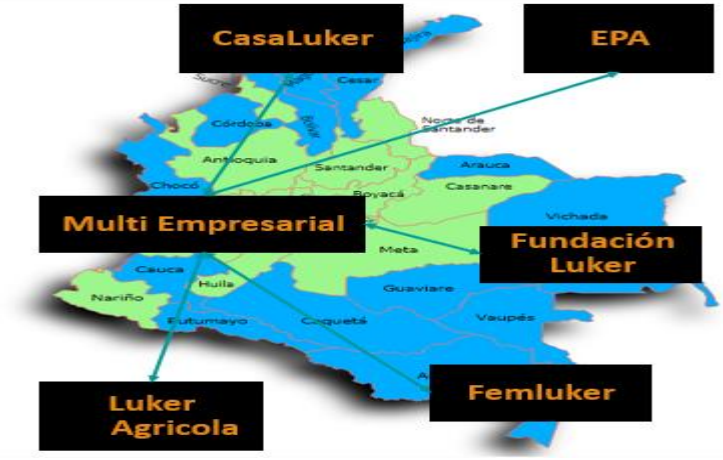
- Diseñar un Marco Gestión de Riesgos de Tecnologías de la Información y Comunicación en entorno multi empresarial de CasaLuker S.A

- Validar el Marco Gestión de Riesgos de Tecnologías de la Información y Comunicación en una de las empresas aliadas a la casa matriz de estudio CasaLuker S.A.

1.6 Alcance

La propuesta contempla la elaboración de un marco general de Gestión de Riesgos de Tecnología de la Información y Comunicación, con base en análisis de datos de herramientas existentes por un periodo de seis meses del portal administrativo de Office 365 de Microsoft, Seguridad perimetral con Fortinet, portal administrativo Sophos en la compañía de Casaluker S.A y las empresas que dependan de la misma área de Tecnología de la información como se observa en **Ilustración 1-3** que involucra Empresa Panameña de alimentos (EPA), Fundación Luker, Luker Agrícola y Fondo de empleados CasaLuker (Femluker). El marco solo se probará en una de las empresas mencionadas en la ciudad de Manizales del departamento de Caldas. El marco metodológico que se implementará no incluye el análisis de los mundos social, personal y material. Se basa en las fases definidas por la multi metodología de Mingers y Brocklesby 1997 como la apreciación, el análisis, la evaluación y la acción (Mingers, 2006).

Ilustración 1-3. Empresas que depende de la misma área de Tecnología de Información



1.7 Metodología

Considerando el contexto de la problemática en términos de la seguridad de la información con características de un entorno multi empresarial según el Core de negocio, datos de las herramientas tecnológicas existentes (portal administrativo de office 365, Consola de firewall o seguridad perimetral y Consola de administración de antivirus Sophos) sobre incidentes o amenazas detectadas y la metodología en la gestión de riesgos de las Tecnologías de la Información y Comunicación, se identifican factores como datos tangibles a los que se pretende analizar para obtener un comportamiento o tendencia que son cuantificables; y una parte cualitativa que está sujeta a las necesidades de los negocios y estimada por los líderes de los procesos para construir un Marco General de Riesgos de Tecnologías de la Información y Comunicación. La metodología que se utilizará para el desarrollo del trabajo es la multi metodología de Mingers y Brocklesby (Mingers, 2006), que involucra métodos cuantitativos y cualitativos para obtener una visión desde diferentes perspectivas del sistema.

La multi metodología fue propuesta por Mingers y Brocklesby (1997), plantea cuatro fases: Apreciación, Análisis, Evaluación y Acción (Mingers, 2006). Se estructuran acorde a los objetivos específicos del trabajo a realizar:

1.7.1 Fase 1 Apreciación (Recolección de datos)

Esta fase comprende la valoración y exploración del estado actual de las diferentes metodologías de la gestión de riesgos en Tecnologías de la Información y Comunicación; y datos de las herramientas tecnológicas existentes del entorno multi empresarial como: el portal administrativo de office 365, Consola de seguridad perimetral firewall Fortinet, consola de administración de antivirus Sophos y demos aplicados en la instancia de recolección. Se plantean las siguientes actividades:

1. Revisión sistemática de literatura acerca de las metodologías de Gestión de Riesgo en Tecnologías de la información y comunicación.
2. Toma de datos (Logs) en cada consola administrativa y el almacenamiento de estos.

1.7.2 Fase 2 Análisis (análisis de datos de campo)

En esta fase se escoge la metodología de Gestión de Riesgos en tecnologías de la información y Comunicación. También las tendencias y comportamientos de los datos recolectados mencionados en la fase 1. Las actividades son las siguientes:

1. Elección de la metodología de Gestión de Riesgos.
2. Analizar los datos para obtener tendencias o comportamientos de seguridad en las empresas.

1.7.3 Fase 3 Evaluación (Construcción de marco)

Esta fase comprende el plan de mejoramiento de la problemática expuesta en el trabajo, mediante la elaboración del diseño del marco de gestión de riesgos, considerando los elementos adquiridos en la fase 1 y 2. La actividad es:

1. Diseño del Marco de Gestión de Riesgo de Tecnología de la información y Comunicación

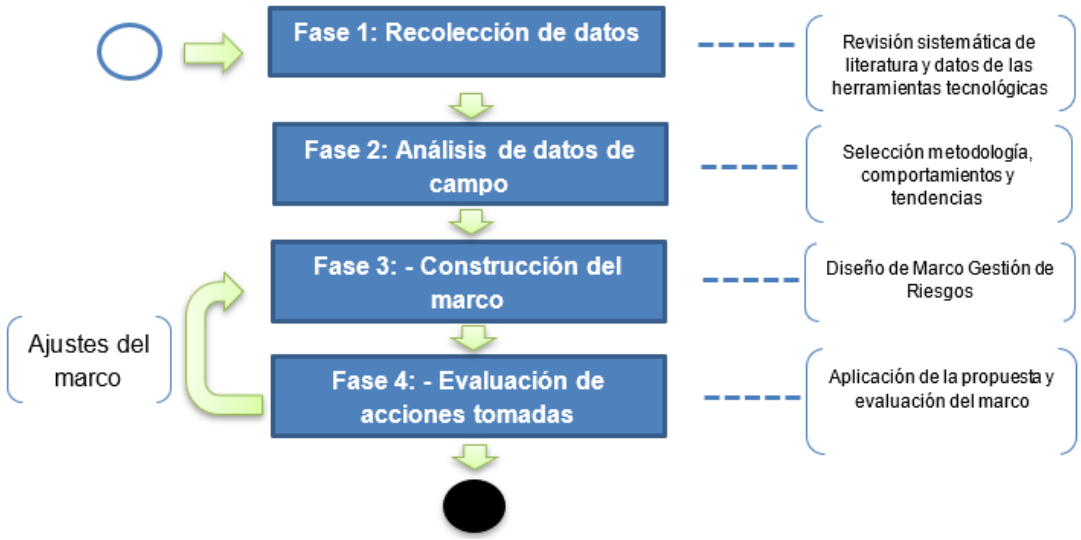
1.7.4 Fase 4 Acción (Evaluación de acciones tomadas)

Se valida el Marco de Gestión de Riesgos de Tecnología de la Información y Comunicación definido en la fase 3, en una de las empresas que depende del área de Tecnología de la Información y Comunicación de CasaLuker. Las actividades son:

1. Aplicación del Marco de Gestión de Riesgos de Tecnología de la Información y Comunicación.
2. Evaluación de los resultados del marco de Gestión de Riesgos con los líderes.

En esta fase se puede establecer ajustes al Marco de Gestión de Riesgo de Tecnología de la información y Comunicación que se construyó en la fase 3. De esta forma, se construye la **Ilustración 1-4** que completa el proceso implementado.

Ilustración 1-4. Fases de la metodología



Fuente: adaptado de Mingers y Brocklesby (1997). (Mingers, 2006)

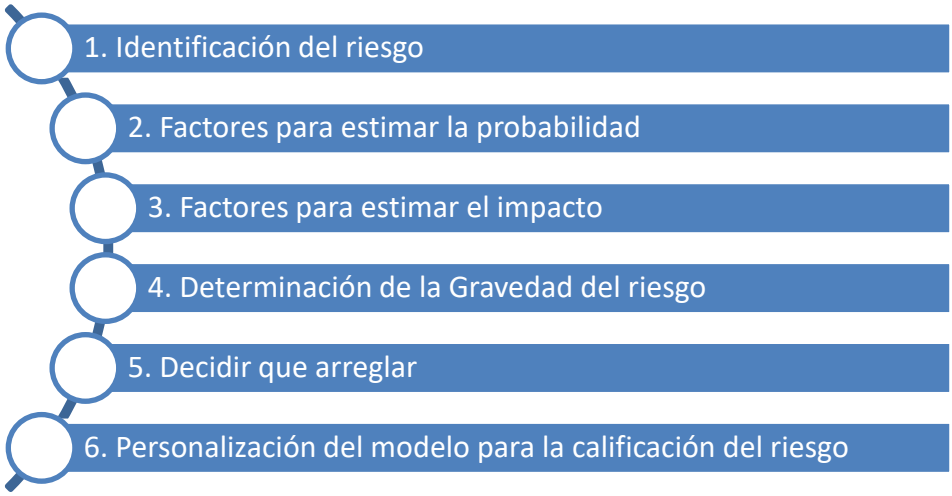
Capítulo 2. OWASP Risk Rating Methodology

Open Web Application Security Proyect, proporciona herramientas y estándares para modelar procesos seguros que mitiguen las vulnerabilidades en las organizaciones (Olivares & Eduardo, n.d.). Estos lineamientos abarcan una serie pasos dentro de los cuales está la identificación de escenarios de posibles riesgos, que puedan causar un deterioro en la productividad de las actividades primordiales para una compañía. La metodología OWASP, enfoca sus esfuerzos hacia los objetivos estratégicos según el Core del negocio y las necesidades que este pudiese tener, con el propósito de generar los controles necesarios que disminuyan ese riesgo, usar el mejor aprovechamiento de recursos tecnológicos y generar esa confianza con relación a la Confidencialidad, Integridad y disponibilidad de la información.

Parte de la estandarización aplicada por esta metodología es buscar los riesgos más relevantes para fortalecer las capacidades técnicas y humanas en el control de los recursos corporativos bajo unos criterios definidos según el impacto para establecer una prioridad. (Williams, n.d.), define OWASP, como un modelo practico para estimar la gravedad de los riesgos, (Munir et al., 2015) indica la simplicidad de como esta metodología abarca una situación de vulnerabilidad y como a partir de ella establece una evaluación del riesgo para mejorar la seguridad.

OWASP maneja un riesgo estándar que es también la base para otras metodologías en donde el Riesgo = Probabilidad * Impacto (Williams, n.d.). Este riesgo debe considerar una serie de pasos que permitan ilustrar las necesidades de la compañía y como estos pueden versen afectados, se estipulan estos pasos en la **Ilustración 2-1**.

Ilustración 2-1. Pasos para determinar y mitigar el Riesgo elaborado a partir de (Owasp, 2013)



2.1 Identificación del Riesgo

Actores que intervienen en el proceso deben recopilar información sobre las amenazas, vulnerabilidades, ataques e impactos que degraden los servicios y a su vez la productividad de la compañía (Munir et al., 2015). Estos escenarios se enfocan hacia los riesgos de Tecnologia de la Información para calificar la importancia y la probabilidad de ocurrencia.

2.2 Factores para estimar la probabilidad (P)

El objeto de este paso es identificar que tan alta es la probabilidad del riesgo en los procesos tecnológicos o sistemas de información dentro del entorno corporativo. Se realiza una clasificación de los factores que está dividido en dos grupos.

2.2.1 Factores de Amenaza (FA)

Este factor consiste en señalar el o los atacantes que verdaderamente puedan hacer eficaz un daño. Se toman criterios como el nivel de habilidad para generar el ataque, que consiste en la capacidad que tiene ese atacante de debilitar el sistema; otro criterio es que propicia realizar el ataque, para estimar el nivel de motivación que por lo general es la obtención de un beneficio, como por ejemplo conseguir las credenciales de acceso a un sistema de

información (Schoenfield, 2015). La oportunidad es un criterio que se enfoca a los recursos que requiere el atacante para hacer efectivo el ataque y por último, el tamaño que hace referencia al grupo de personas que afectaría el ataque en el entorno corporativo (Munir et al., 2015) (Williams, n.d.). Estos criterios se evalúan bajo una escala de 0 a 9, se selecciona una calificación **Ilustración 2-2** que permita estimar la probabilidad a nivel de amenaza.

Ilustración 2-2. Factores de agente de amenaza

Factores de agentes de amenaza			
Nivel de Habilidad	**Motivación**	**Oportunidad**	**Tamaño**
0-	0-	0- Se requiere acceso total o recursos costosos	0-
1- Sin habilidades técnicas	1- Recompensa baja o nula	1-	1-
2-	2-	2-	2- Administradores de sistemas
3- Algunas habilidades técnicas	3-	3-	3-
4-	4- Recompensa posible	4- Se requiere acceso o recursos especiales	4- Usuarios Intranet
5- Usuario avanzado en computadores	5-	5-	5- Socios
6- Habilidades de programación y redes	6-	6-	6- Usuarios autenticados
7-	7-	7- Se requiere algún acceso o recursos	7-
8-	8-	8-	8-
9- Habilidades de penetración de seguridad	9- Recompensa alta	9- No se requiere acceso o recursos	9- Usuario de Internet anónimos

Fuente: elaborado a partir de (Williams, n.d.)

2.2.2 Factores de Vulnerabilidad (FV)

Tiene por ende establecer, como el atacante descubre la debilidad del sistema y a partir de ella, saca tajada en beneficio propio. Este análisis se lleva a cabo mediante perspectivas relacionadas con la facilidad de descubrimiento, en la que se infiere que tan sencillo es para el atacante poder reconocer una deficiencia de seguridad, que simplicidad puede tener para explotar esa falla (facilidad de explotación) y que tan familiarizado podría estar con el atacante (conciencia) (Schoenfield, 2015). También se evalúa la detección de intrusiones, habilidad que se tiene para ver los comportamientos de lo que podría ser anormal dentro de un sistema, para lo cual se establece que posibilidad hay de detectar una vulnerabilidad (Williams, n.d.). Estos criterios se evalúan bajo una escala de 0 a 9 como se observa en la **Ilustración 2-3**, se selecciona la calificación que permitirá realizar el computo para estimar la probabilidad.

Ilustración 2-3. Factores de Vulnerabilidad

Factores de vulnerabilidad			
Facilidad de descubrimiento	**Facilidad de explotación**	**Conciencia**	**Detección de Intrusiones**
0-	0-	0-	0-
1- Practicamente Imposible	1- Teórico	1- Desconocido	1- Detección activa en la aplicación
2-	2-	2-	2-
3- Difícil	3- Difícil	3-	3- Registrada y revisada
4-	4-	4- Oculto	4-
5-	5- Fácil	5-	5-
6-	6-	6- Obvio	6-
7- Fácil	7-	7-	7-
8-	8-	8-	8- Registrada sin revisión
9- Herramientas automatizadas disponibles	9- Herramientas automatizadas disponibles	9- Conocimiento público	9- No registrada

Fuente: elaborado a partir de (Williams, n.d.)

Una vez establecida la calificación de cada uno de los criterios, se establece el promedio de la sumatoria de los factores agente de amenaza y vulnerabilidad. El resultado del cálculo nos permitirá definir la probabilidad de ocurrencia con base en la **Tabla 2-1** del escenario de riesgo.

Tabla 2-1. Probabilidad de ocurrencia

Rango	Severidad
Entre 0 y 3	Bajo
Entre 3 y 6	Medio
Entre 6 y 9	Alto o Critico

Fuente: elaborado a partir de (Williams, n.d.)

2.3 Factores para estimar el Impacto (I)

El impacto es el efecto que puede producir esa vulnerabilidad en el entorno corporativo y se clasifica en dos tipos.

2.3.1 Impacto Técnico (IT)

Este está enfocado al sistema o aplicación que establece que tan fuerte puede ser el daño en la ejecución de las operaciones, como este afecta en términos de seguridad la triada (confidencialidad, integridad y disponibilidad) al igual que la responsabilidad (Munir et al., 2015). La pérdida de confidencialidad implica cuantos datos se podrían difundir y que tan

doloroso sería para la organización, en cuanto a la perdida de integridad el enfoque es hacia cuantos datos se podrían echar a perder y el nivel daño de estos. La disponibilidad indica cuantos servicios se comprometerían y que tan indispensables son. Por último, la perdida de responsabilidad se orienta hacia el rastreo de las acciones de los agentes de amenaza. Estos criterios se evalúan bajo una escala de 0 a 9, se selecciona la calificación que permitirá realizar el computo considerando la **Ilustración 2-4** para estimar el impacto técnico.

Ilustración 2-4 Impacto técnico

Impacto Técnico			
Pérdida de confidencialidad	**Pérdida de integridad**	**Pérdida de disponibilidad**	**Pérdida de responsabilidad**
0-	0-	0-	0-
1-	1- Datos mínimos levemente corruptos	1- Servicios secundarios mínimos interrumpidos	1- Totalmente rastreable
2- Información mínima no confidencial divulgada	2-	2-	2-
3-	3- Minímo de datos muy corruptos	3-	3-
4-	4-	4-	4-
5-	5- Datos extensos ligeramente corruptos	5- Servicios primarios mínimos interrumpidos - servicios secundarios extensos interrumpidos	5-
6- Información mínima crítica divulgada - Divulgación de datos no confidenciales extensos	6-	6-	6-
7- Divulgación de datos criticos extensos	7- Datos extensos muy corruptos	7- Servicios primarios extensos interrumpidos	7- Posiblemente rastreable
8-	8-	8-	8-
9- Divulgación de todos los datos	9- Todos los datos totalmente corruptos	9- Todos los servicios completamente perdidos	9- Completamente anónimo

Fuente: elaborado a partir de (Williams, n.d.)

2.3.2 Impacto Comercial (IC)

Este impacto es prácticamente lo que podría soportar las inversiones de las empresas en recursos tecnológicos, puesto que es apalancada por los factores de riesgos y la importancia de estos en respaldar las operaciones (Williams, n.d.), que generen ese valor de productividad para los dueños o accionistas. Por tanto, se evalúa el daño financiero enfocado hacia las perdidas por la amenaza, la reputación que implica el resultado del daño en la imagen de la empresa ante sus competidores y lo más importante, sus clientes. También se evalúa el incumplimiento y la violación de la privacidad en términos de cuanta información personal se divulgaría. Se establece la calificación en el rango de 0 a 9 considerando **Ilustración 2-5** para computar los datos del impacto comercial.

Ilustración 2-5. Impacto Comercial

Impacto Comercial			
Daño Financiero	**Daño a la reputación**	**Incumplimiento**	**Violación de la privacidad**
0-	0-	0-	0-
1- Menos que el costo de reparar la vulnerabilidad	1- Daño mínimo	1-	1-
2-	2-	2- Violación menor	2-
3- Efecto menor en la ganancia anual	3-	3-	3- Un individuo
4-	4- Perdida de cuentas importantes	4-	4-
5-	5- Perdida de buena voluntad	5- Violación clara	5- Ciento de personas
6-	6-	6-	6-
7- Efecto significativo en la ganancia anual	7-	7- Violación alta perfil	7- Miles de personas
8-	8-	8-	8-
9- Quiebra	9- Daño a la marca	9-	9- Millones de personas

Fuente: elaborado a partir de (Williams, n.d.)

2.4 Determinación de la Gravedad del Riesgo (GR)

La gravedad del riesgo es la combinación del paso 2.2 y 2.3 (probabilidad e impacto) (Munir et al., 2015). Los niveles de riesgo son bajo, medio y alto que también se le conoce como crítico. La **Tabla 2-2** representa la gravedad del riesgo.

Tabla 2-2 Calificación de la gravedad del riesgo

Rango	Nivel del Riesgo
Entre 0 y < 3	Bajo
Entre 3 y < 6	Medio
Entre 6 y < 9	Alto o Critico

Fuente: elaborado a partir de (Williams, n.d.)

Considerando lo anterior, se establece un cruce de los resultados de la probabilidad e impacto con base en la **Ilustración 2-6**.

Ilustración 2-6. Severidad General del Riesgo

Severidad General del riesgo = Probabilidad x Impacto				
Impacto	Alto	Medio	Alto	Critico
	Medio	Bajo	Medio	Alto
	Bajo	Note	Bajo	Medio
		Bajo	Medio	Alto
	Probabilidad			

Fuente: tomado de (Williams, n.d.)

Cada escenario de riesgo se evalúa mediante este proceso para definir la gravedad del riesgo y ver que acciones se pueden ejecutar en la mitigación de esa eventualidad. Por tanto, si el resultado de la probabilidad da como resultado Medio, previamente estableciendo el cálculo de los factores de amenaza y vulnerabilidad sobre el número de factores de probabilidad; y el impacto es alto, previamente estableciendo el cálculo del impacto comercial y técnico sobre el número de factores de impacto, se podría concluir que la gravedad del riesgo es alta. Se consolida el proceso en **Ilustración 2-7**.

Ilustración 2-7. Consolidación proceso gravedad del riesgo

<table>
<tr><td>$P = \frac{\sum FA + \sum FV}{n}$</td><td rowspan="2">Se compara el resultado con:
<table><tr><td>Entre 0 y < 3</td><td>Bajo</td></tr><tr><td>Entre 3 y < 6</td><td>Medio</td></tr><tr><td>Entre 6 y < 9</td><td>Alto o Critico</td></tr></table>
Esto puede ser personalizado según criterio estipulado por los evaluadores</td><td>Para el ejemplo considerado la probabilidad es “Medio”</td></tr>
<tr><td>$I = \frac{\sum IT + \sum IC}{n}$</td><td>Para el ejemplo considerado el impacto es “Alto”</td></tr>
<tr><td colspan="2">GR
<table><tr><td colspan="5">Severidad General del riesgo = Probabilidad x Impacto</td></tr><tr><td rowspan="3">Impacto</td><td>Alto</td><td>Medio</td><td>Alto</td><td>Critico</td></tr><tr><td>Medio</td><td>Bajo</td><td>Medio</td><td>Alto</td></tr><tr><td>Bajo</td><td>Note</td><td>Bajo</td><td>Medio</td></tr><tr><td></td><td>Bajo</td><td>Medio</td><td>Bajo</td></tr><tr><td></td><td colspan="4">Probabilidad</td></tr></table></td><td>Al aplicar el cruce entre impacto y probabilidad se concluye que la gravedad del riesgo es “Alto”.</td></tr>
</table>

Fuente: elaborado a partir de (Williams, n.d.)

La experiencia y el conocimiento de los procesos organizacionales y tecnológicos permitirán ser más asertivos para obtener la calificación de la gravedad del riesgo en las vulnerabilidades y amenazas del entorno, lo que hace que el proceso tenga la orientación correcta.

2.5 Decidir que arreglar

La determinación del riesgo proporciona un insumo muy importante a la organización y en especial a sus dirigentes. Este esquema brinda una ruta de trabajo mucho más priorizado, de tal forma que las decisiones de sus dirigentes son más sencillas de aclarar en el establecimiento de objetivos, para enfocar los esfuerzos en diferentes capaz de seguridad y recursos tecnológicos necesarios para la mitigación del riesgo.

2.6 Personalización del modelo para la calificación del riesgo

Los riesgos para una organización y sus dirigentes pueden estar atados a prejuicios calificativos, puesto que para cada área se respalda la importancia de sus procesos y estos pueden prevalecer sobre otros. Por tanto, es necesario la integración entre las diferentes áreas para tipificar en gran escala corporativa los verdaderos riesgos. En esta parte, el evaluador debe generar un comparativo entre el grupo de expertos y los resultados arrojados por el modelo, de tal forma que se puedan aplicar los ajustes necesarios para que el efecto sea mucho más asertivo (Williams, n.d.). También se puede aplicar ponderaciones y costos asociados a la consecuencia de generarse la efectividad de un evento negativo.

La metodología OWASP permite definir criterios enfocados hacia las mejores prácticas organizacionales, en la creación de la línea base en la seguridad de la información para que conceptos como la confidencialidad, integridad y disponibilidad de la información tengan una menor vulnerabilidad a las amenazas constantes del medio. El objetivo es robustecer la seguridad mediante la provisión de esquemas basado en el análisis comprometido, por cada uno de los actores del sistema. Esto implica la vinculación de los recursos humanos y tecnológicos para el cumplimiento de las acciones necesarias en beneficio de las empresas.

Capítulo 3. Descripción de herramientas tecnológicas existentes y las principales amenazas detectadas

Con los recursos tecnológicos disponibles de una organización se puede contribuir a la definición de un esquema metodológico basado en hechos de los eventos registrados que puedan condicionar una estructura de seguridad enfocada a la información de la compañía sin dejar a un lado los objetivos estratégicos del negocio.

Un evento atípico en la recolección de datos es la problemática mundial relacionado con la pandemia (COVID-19) puesto que ha cambiado la forma de ejecutar las labores de los colaborares en las organizaciones modificando sus sitios de trabajo hacia los hogares. Sin embargo, las herramientas mencionadas en el presente documento contribuyen en el monitoreo constante de las acciones que se ejecutan como parte de su labor dentro del entorno multi empresarial de CasaLuker. Se describe a continuación las herramientas de las que se obtuvieron datos:

3.1 Portal Administrativo Microsoft Office 365

Al adquirir un licenciamiento corporativo de Microsoft, se obtiene un acceso a la administración de opciones sobre las herramientas o software que este posee, una de ellas es el Centro y Seguridad de cumplimiento (Centro de Seguridad y Cumplimiento - Service Descriptions | Microsoft Docs, n.d.). Desde allí se puede obtener registros sobre el comportamiento de las aplicaciones de Microsoft como: Detecciones de correo no

deseado, Detecciones de suplantación de identidad, protección contra amenazas, flujo de correo entre otros.

Los demás reportes que se encuentran en la plataforma están referenciados a la usabilidad y rendimiento del sistema como consultas especificas orientadas a la gestión (Centro de Seguridad y Cumplimiento - Service Descriptions | Microsoft Docs, n.d.). Los puntos señalados se remiten a la seguridad del flujo de información sobre la plataforma de correo corporativo de todos los usuarios activos de la organización.

Cada de una de estas herramientas suministran datos que son almacenados hasta por 90 días y advierten sobre el funcionamiento de los recursos que son asignados a los usuarios finales como lo es una cuenta de correo electrónico, que al pasar de los años se ha convertido en un medio de gran importancia para respaldar acciones correspondientes al cargo desempeñado por el colaborador. Por tanto, es un recurso necesario en la ejecución diaria de las operaciones organizativas. Ahora, una cuenta de correo puede contener información de alto nivel que, en manos de la competencia, hackers u otros podrían generar algún trauma en la gestión de la información como perdida, bloqueo de sistemas, uso de esta para fines comerciales y delictivos que pondrían en vilo operaciones estratégicas, pérdida de valor, imagen y confianza ante los clientes y/o proveedores. Se recopilan datos (Logs) por un periodo de 7 meses, iniciando desde el 15 septiembre del 2.020 al 30 de abril del 2.021 de las siguientes opciones:

3.1.1 Malware detectado

Malware, es un término referenciado a programas o aplicaciones maliciosas que deterioran los servicios e infectan equipos cómputo con subrutinas para obtener accesos no autorizados y generar sustracción de claves de las aplicaciones corporativas o personales de los usuarios (Fuentes, 2008). También disminuyen el rendimiento del equipo computo afectando las labores diarias, robo parcial o total de información por solo causar un daño o generar algún tipo de extorción, entre otros eventos (Microsoft, 2021d). Microsoft, bajo su documentación categoriza los Malware como se visualiza en la siguiente **Tabla 3-1**.

Tabla 3-1. Categorización Malware

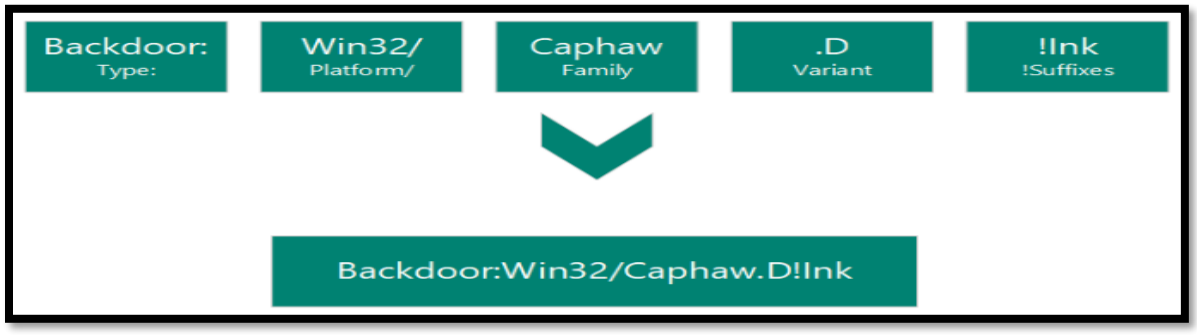
Amenaza	Descripción
Puerta trasera	Proporciona acceso remoto y control de un equipo de cómputo a personas con conocimiento en programación para ejecutar acciones maliciosas (Hackers)
Descargador	Genera descarga de otro Malware en el equipo computo. Requiere de acceso a internet.
Dropper	Este instala archivos de Malware en el equipo computo. No requiere de internet
Exploit	Con base en las vulnerabilidades del software este usa partes de código para generar un acceso a dispositivo y así poder ejecutar tareas especificas
Hacktool	Esta herramienta se utiliza para el acceso a un equipo de cómputo sin tener la autorización.
Virus de Macro	Este Malware se extiende por medio de documentos como la suite de office 365 (Word, Excel, PowerPoint, otros) que se encuentran infectados.
Ofuscator	El código del programa malicioso es difícil de detectar al igual que su eliminación
Administrador de contraseñas	Captura la debilidad de los usuarios referenciado a los datos sensibles como lo son las cuentas de acceso y claves mediante un registro de las pulsaciones de las teclas utilizadas. En general recopila datos del usuario.
Rasomware	Cifra o modifica los archivos para que el usuario no los pueda utilizar. Por lo general generan extorción para que el usuario pague y así recupere la información.
Software de seguridad no deseado	Su fin es mostrar alertas de amenazas que quizás ni existan en el dispositivo. Actúa como un antivirus o programa de protección, pero no lo es.
Troyano	Tiene como propósito robar información personal, dar acceso a los atacantes o descargar de otros Malware. Este no se propaga por sí mismo como lo hace un gusano.
Clicker de troyano	Este genera clic de forma automática en anuncios, sitios web entre otros así generar acciones como instalación de software en el equipo computo
Gusano	Este se propaga fácilmente por diferentes medios como correo electrónico, archivos compartidos o medios de trabajo colaborativo entre otras formas

Fuente: tomado de (Microsoft, 2021d)

De esta forma, Microsoft genera una nomenclatura para la identificación de estas amenazas como se visualiza en la **Ilustración 3-1**, en la que el tipo se refiere a lo que realiza el Malware en el equipo computo como lo son los virus, gusanos, troyanos, puertas

traseras, Rasomware, spyware, adware entre otros. La plataforma significa el sistema operativo (Windows, Android, MasOS, otros), el lenguaje de programación (ABAP, HTML, JAVA, Python, PHP, JS entre otros) o el formato del archivo (XLM, ASX, SWF, entre otros) con el que el Malware funciona. La familia corresponde a las características semejantes y por las cuales se agrupa el Malware y con la carta variant se indica la versión de forma secuencial. Por último, están los sufijos (.dll, .dam, .gen, .worm, @mm, entre otros) que suministran más datos sobre la amenaza. Por ejemplo, ".gen" indica que el Malware se detecta con una firma genérica (Microsoft, 2021d).

Ilustración 3-1 Nomenclatura Malware



Fuente: tomado de (Microsoft, 2021d)

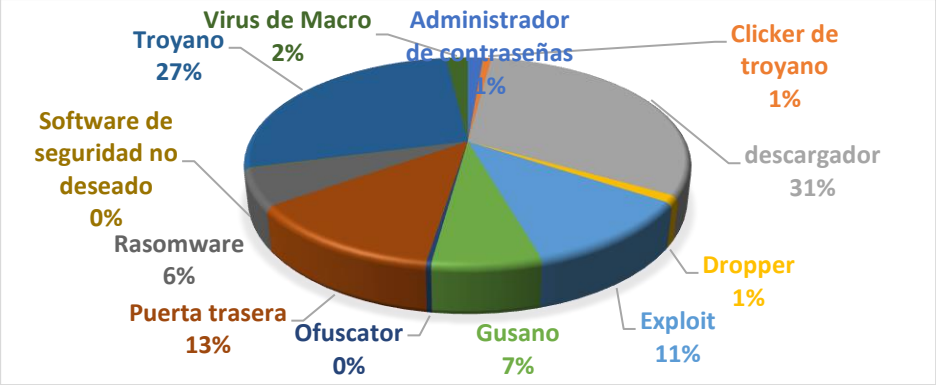
La **Ilustración 3-2** muestra los registros que se pueden obtener, para identificar las amenazas, las incidencias o cantidades según la empresa y una visual sobre un comportamiento de los ataques. Se adiciona una columna para identificar la categoría del Malware con base en la documentación de Microsoft (Microsoft, 2021c).

Ilustración 3-2. Registros Logs Malware

origin_times	sender_addr	recipient_ad	Empresa	message_sul	total_bytes	message_id	network_me	original_clie	directionalit	event_type	filename	malware_name	
2020-06-24 0	katewright_(	lukercacao@casaluker.co		Failed DHL D	553455	<93f1a92292	7c1f0238-996	178.63.13.15	Incoming	Malware	Delivery Not	W32/MSIL_Agent.BLL.gen!Eldo	
2020-06-24 1	ilhan@betat	ccastano@casaluker.com.		"Audio To Co	16995	<hWsL3iSbiE	74f42b40-808	74.208.4.196	Incoming	Malware	##########	HTML/Refresh.G!MSR	
2020-06-24 1	roselmos@o	vjimenezfundacion@casa		Admistia Cor	228427	<DM6PR17M	ad7f4ebc-18	40.92.21.102	Incoming	Malware	Acuerdo De	js	
2020-06-24 1	Lanny.Mane	lukercacao@casaluker.co		DHL: Shipme	699960	<ca0ecce980	efb56010-62	95.217.94.19	Incoming	Malware	shipment do	Malicious Payload	
2020-06-24 1	Lanny.Mane	lukereu@casaluker.com.c		DHL: Shipme	699988	<1042975d45	5d3a51d7-15	95.217.94.19	Incoming	Malware	shipment do	Malicious Payload	
2020-06-25 0	citaspruebas	gerenciafemluker@casalu		Usted ha sid	87836	<ZL1X20Y3-S	2321c2ff-759	##########	Incoming	Malware	citacion prue	PDF/Trojan.SBSS-6	

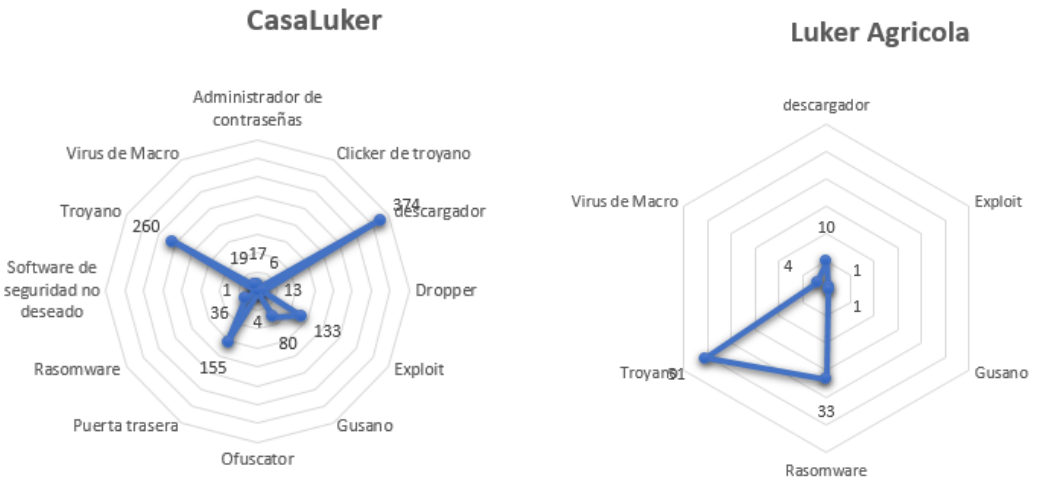
Se obtuvieron 1259 registros, en donde el 31% corresponde a la categoría de "descargador", seguido de un 27% "Troyano" como se detalla en la **Ilustración 3-3**.

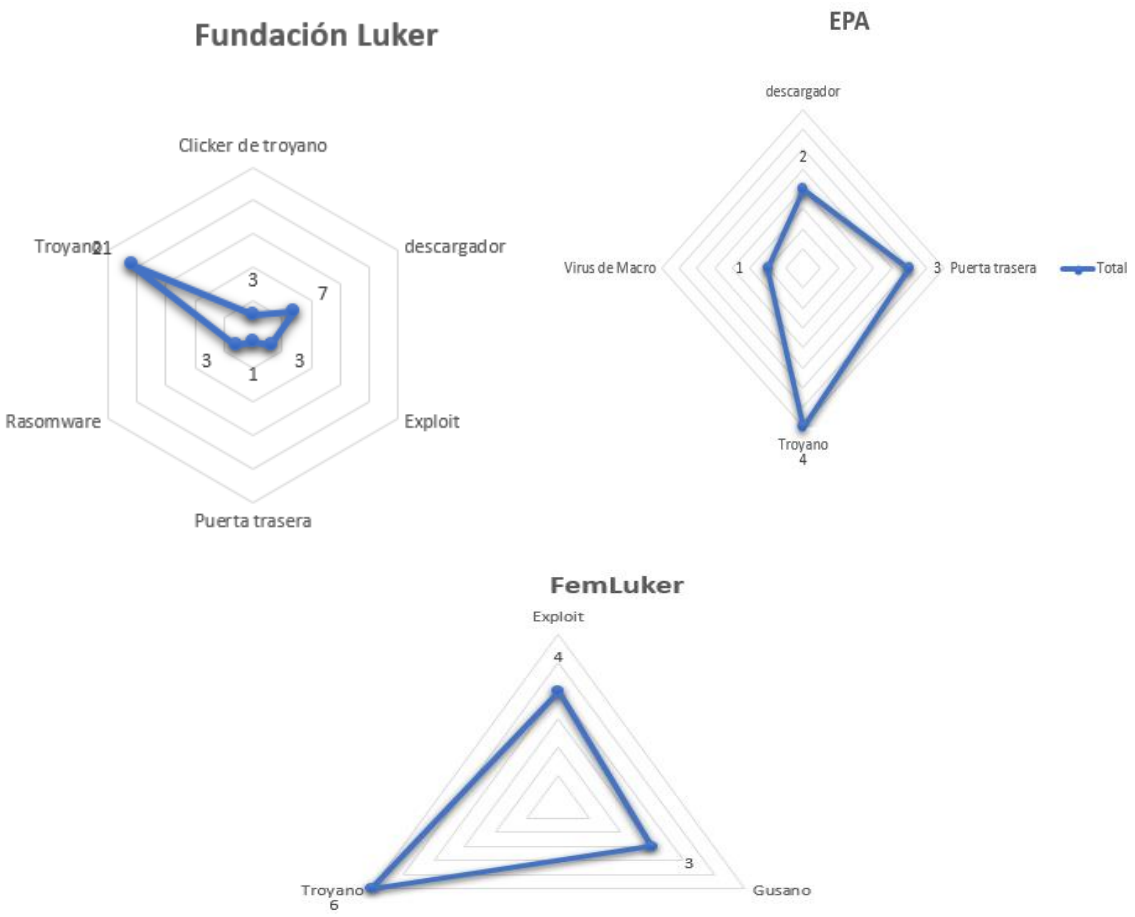
Ilustración 3-3. Malware detectado



CasaLuker tiene una población de 830 equipos computo (Escritorio – Portátiles - Servidores) seguida de Luker Agricola con 58, Fundación Luker 45, EPA 30 y FemLuker (Fondo de empleados) 6. La **Ilustración 3-4** muestra el comportamiento de estas amenazas según la empresa del entorno multi empresarial. Las amenazas más evidentes para CasaLuker están referenciadas en descargador, troyano y puerta trasera; para Luker Agricola, sus incidencias están más evidenciadas en amenazas de tipo troyano seguido de evento de Rasomware que podría ocasionar traumatismos por perdida de información del usuario sobre el equipo computo. Fundación Luker, también se evidencia los eventos de tipo troyano al igual que para la empresa EPA y Femluker.

Ilustración 3-4. Malware por empresa





3.1.2 Suplantación de identidad (Email Spoofing)

Email Spoofing, consiste en la creación de mensajes mediante remitentes falsos con el propósito de hacer que el usuario divulgue la información personal o corporativa, datos sobre información bancaria, contraseñas, descarga de software malicioso, entre otros (Microsoft, 2021c). Es una técnica de phishing, un ataque programado para obtener datos (Benavides et al., 2020).

Microsoft proporciona mecanismos de protección como anti-spoofing que chequea los correos electrónicos mediante Exchange Online Protection (EOP), de tal forma que analiza el encabezado en el cuerpo del mensaje para identificar si se refiere a una cuenta falsificada para proceder con el bloqueo (Microsoft, 2021c).

La **Ilustración 3-5**, contiene un ejemplo del resultado de los registros solicitados a la consola de administración de office 365. Se obtuvieron 3190 registros que cruzados con las bases de datos de empleados se puede consolidar la empresa a la que corresponde. Estos logs están disponibles por un periodo no superior a 3 meses.

Ilustración 3-5. Registros suplantación de identidad

TenantId	DateUtc	Source	Verdict	P2Sender	PtrDomains	ConnectingIp
8d8555e4-8189-43f3-98	25/06/2020	SpoofMai	CaughtAsSpan	smgaleano@lukerchocolate.com	salesforce.com	13.110.14.0/24
8d8555e4-8189-43f3-98	25/06/2020	SpoofMai	GoodMail	facturacionfunza@casaluker.com.co	google.com	209.85.160.0/24
8d8555e4-8189-43f3-98	25/06/2020	SpoofMai	GoodMail	facturacionfunza@casaluker.com.co	google.com	209.85.222.0/24
8d8555e4-8189-43f3-98	25/06/2020	SpoofMai	GoodMail	ase-com-femluker@casaluker.com.co	outlook.com	104.47.38.0/24
8d8555e4-8189-43f3-98	25/06/2020	SpoofMai	GoodMail	ase-com-femluker@casaluker.com.co	outlook.com	104.47.46.0/24
8d8555e4-8189-43f3-98	25/06/2020	SpoofMai	GoodMail	ase-com-femluker@casaluker.com.co	outlook.com	104.47.55.0/24
8d8555e4-8189-43f3-98	25/06/2020	SpoofMai	GoodMail	ase-com-femluker@casaluker.com.co	outlook.com	104.47.57.0/24
8d8555e4-8189-43f3-98	25/06/2020	SpoofMai	CaughtAsSpan	arodriguez@lukerchocolate.com	salesforce.com	13.110.14.0/24
8d8555e4-8189-43f3-98	26/06/2020	SpoofMai	GoodMail	notifications@monday.com	monday.com	167.89.105.0/24
8d8555e4-8189-43f3-98	26/06/2020	SpoofMai	CaughtAsSpan	smgaleano@lukerchocolate.com	salesforce.com	13.110.14.0/24
8d8555e4-8189-43f3-98	26/06/2020	SpoofMai	GoodMail	aperilla@casaluker.com.co	outlook.com	40.107.68.0/24
8d8555e4-8189-43f3-98	26/06/2020	SpoofMai	CaughtAsSpan	ase-com-femluker@casaluker.com.co	outlook.com	40.92.9.0/24
8d8555e4-8189-43f3-98	26/06/2020	SpoofMai	GoodMail	sst@lukeragricola.com.co	outlook.com	104.47.36.0/24
8d8555e4-8189-43f3-98	26/06/2020	SpoofMai	CaughtAsSpan	arodriguez@lukerchocolate.com	salesforce.com	13.110.14.0/24
8d8555e4-8189-43f3-98	26/06/2020	SpoofMai	GoodMail	comunicacionesinternasb2b@lukerchocolate.com	outlook.com	104.47.45.0/24
8d8555e4-8189-43f3-98	26/06/2020	SpoofMai	GoodMail	comunicacionesinternasb2b@lukerchocolate.com	outlook.com	104.47.55.0/24
8d8555e4-8189-43f3-98	26/06/2020	SpoofMai	GoodMail	comunicacionesinternasb2b@lukerchocolate.com	outlook.com	40.107.92.0/24

El anti-spoofing, captura correos electrónicos sospechosos, aplica un análisis bajo métodos de reputación y autenticación para declarar el correo como un Spam o permitir el acceso de este al colaborador de la compañía. CasaLuker tiene la mayor parte de correos capturados según la **Ilustración 3-6** por la gran cantidad de usuarios que usan el servicio de correo electrónico a diferencia de la empresa LukerAgricola que no tiene correos detecciones como Spam. Este tipo de datos permite generar en la compañía conciencia sobre las amenazas latentes y como poder prevenirlas.

El proceso iniciado en la captura de registros (logs) fue desde el mes de septiembre 2020, se evidencia el incremento de la revisión de correos por posible suplantación de identidad y muchos de ellos categorizados como Spam como se aprecia en la **Ilustración 3-7**.

Ilustración 3-6. Distribucion evento suplantación identidad por empresa

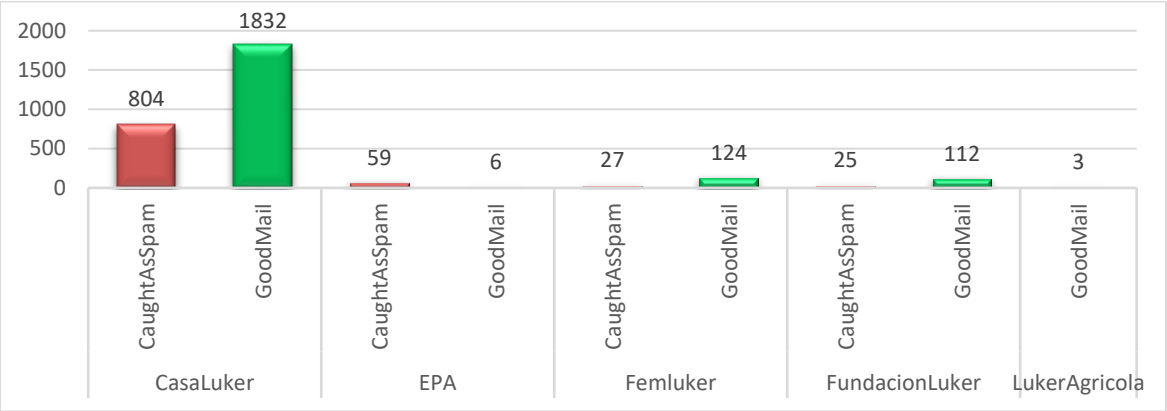
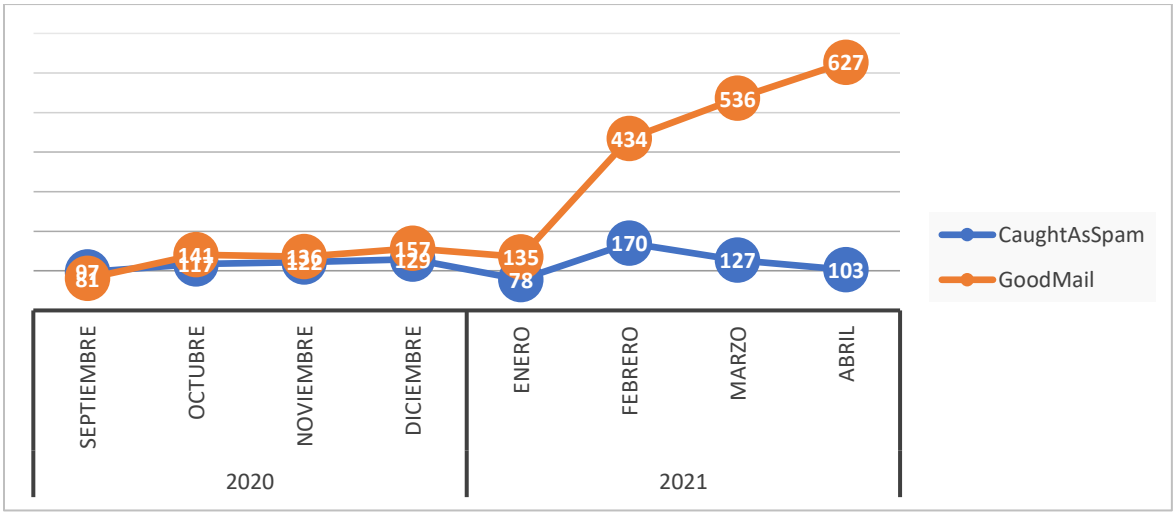


Ilustración 3-7. Revisión correos por suplantación de identidad



3.1.3 Detecciones de Spam

Mediante la herramienta Spam Content Filtered se puede ejercer una barrera de protección ante el flujo de correos mediante un análisis que aplica en cada proceso sobre información publicitaria, correos de dudosa procedencia, alguno de ellos con técnicas de phishing o Malware que pueden comprometer el funcionamiento y/o rendimiento de un equipo computo, perdida de datos del correo y en algunos casos el control de la cuenta (Microsoft, 2021a). De esta manera, ponen en riesgo la operatividad de la organización puesto que

pueden declarar el dominio corporativo dentro de una lista negra, sacarla de esta es un proceso engorroso, demorado ante las necesidades de comunicación de la empresa.

Microsoft Office 365 usa Exchange Online Protection (EOP) que al igual que Email Spoofing proporciona una revisión del correo, delimitando el acceso a posibles eventos en las que la empresa se pueda ver comprometida. El Log recolectado de esta herramienta tiene 101.799 registros donde la empresa CasaLuker como se muestra en la **Ilustración 3-8** tiene la mayor cantidad con un 86% seguido de la Fundación Luker con un 7%. La procedencia de estos correos catalogados como spam con base en la **Ilustración 3-9** corresponde a estados Unidos como uno de los países que más envía este tipo de correo seguida de Francia. La **Ilustración 3-10** permite visualizar como desde la toma de la muestra ha estado aumentando la cantidad de correos recibidos y que la herramienta cataloga como peligrosos. Por tanto, este tipo de medios de comunicación se han convertido en una herramienta fundamental de las empresas debido a la virtualidad para apalancar sus procesos operativos.

Ilustración 3-8. Detecciones de Spam por empresa

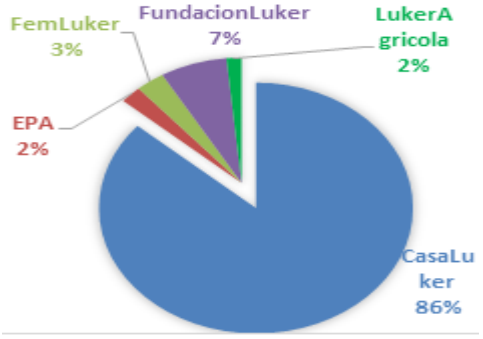


Ilustración 3-9. Top 10 procedencia de Spam

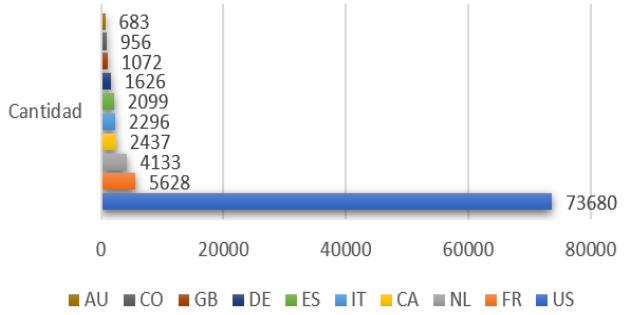
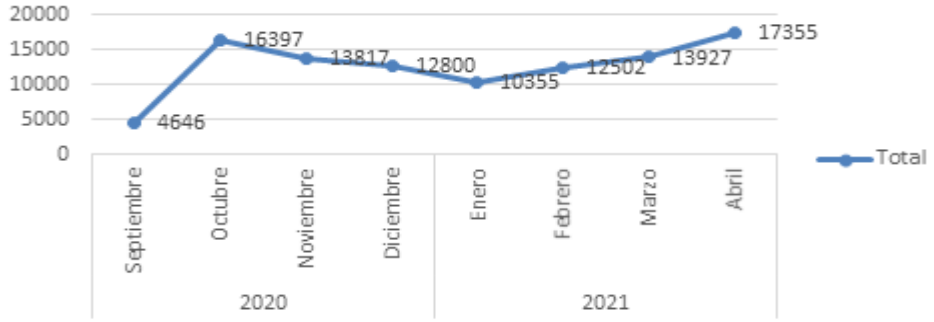


Ilustración 3-10. Cantidad de Spam por mes



El anti-Spam es configurable mediante la consola proporcionada por la herramienta de Microsoft office 365, para lo cual se puede establecer criterios en asumir posturas más concretas de lo que pudiese ser algo malicioso y no impedir el acceso de correos que la empresa realmente requiera.

3.1.4 Consola Administrativa Antivirus “Sophos”

Sophos Endpoint Security es una herramienta que permite brindar una barrera de protección y seguridad ante las amenazas informáticas latentes como virus, malwares o de forma general programas maliciosos. El avance de la tecnología ha permitido evolucionar en este tipo de soluciones ya que los agentes de Sophos en los equipos computo sincronizan hacia la nube donde se encuentra la administración de la plataforma, de tal manera que permite actualizar los dispositivos desde cualquier lugar en el que se encuentren los usuarios, con la condición de que estén conectados a la internet para el correcto funcionamiento (Sophos, 2012). Esta herramienta permite establecer criterios de

administración como bloqueos USB, políticas de protección de navegación en sitios de baja reputación, escaneo en tiempo real y generación de alertas sobre las incidencias que permita concentrar la atención de los administradores del área de la Tecnología de la Información.

Los logs son almacenados por la consola de Sophos hasta por 90 días, con estos registros se obtiene tendencias de amenazas sobre las empresas, lo cual contribuye a generar procedimientos, cultura y políticas hacia la gestión del riesgo en la seguridad de la información; creando así, una sinergia de protección en todas las unidades de trabajo empresarial.

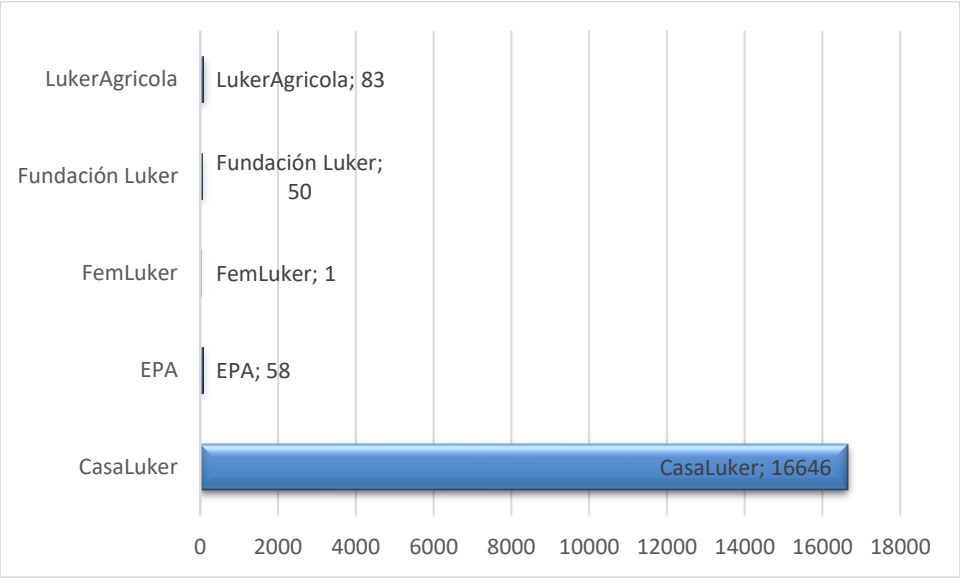
La **Ilustración 3-11**. Registros consola Sophos de Malware muestra los eventos diarios, las amenazas, equipos afectados, usuarios que, combinados con la base de datos de nómina, se puede establecer la empresa a la que pertenecen y como está pueda adoptar una mejora en sus procesos.

Ilustración 3-11. Registros consola Sophos de Malware

When	Threat Name	Threat Path	Event
2020-07-01T16:19:57Z	Malâˆ•HTMLGen-A	abdurantom.com	Access was blocked to "abdurantom.com" because of "Malâˆ•HTMLG
2020-07-01T16:26:11Z	Malâˆ•HTMLGen-A	abdurantom.com	Access was blocked to "abdurantom.com" because of "Malâˆ•HTMLG
2020-07-01T16:27:06Z	Malâˆ•HTMLGen-A	abdurantom.com	Access was blocked to "abdurantom.com" because of "Malâˆ•HTMLG
2020-07-01T17:23:14Z	Malâˆ•HTMLGen-A	www.topdisplaynetwork.com	Access was blocked to "www.topdisplaynetwork.com" because of "M
2020-07-01T17:23:17Z	Malâˆ•HTMLGen-A	www.topdisplaynetwork.com	Access was blocked to "www.topdisplaynetwork.com" because of "M
2020-07-01T17:23:26Z	Malâˆ•HTMLGen-A	www.topdisplaynetwork.com	Access was blocked to "www.topdisplaynetwork.com" because of "M
2020-07-01T17:23:34Z	Malâˆ•HTMLGen-A	www.topdisplaynetwork.com	Access was blocked to "www.topdisplaynetwork.com" because of "M

Se obtienen 16838 registros sobre eventos detectados y considerados como maliciosos, en la que la empresa CasaLuker por su gran cantidad de equipos computo lleva la primera posición con 16646 eventos seguido de la empresa Luker Agricola con 83 eventos como se ilustra en la **Ilustración 3-12**

Ilustración 3-12. Consola Sophos - Malware por empresa



Los eventos que la herramienta detecta son bajo las categorías estipuladas por la consola administrativa de Sophos (Sophos Central Admin, 2021), la **Tabla 3-2** contiene esa clasificación de los registros obtenidos.

Tabla 3-2. Categoría Malware según Sophos

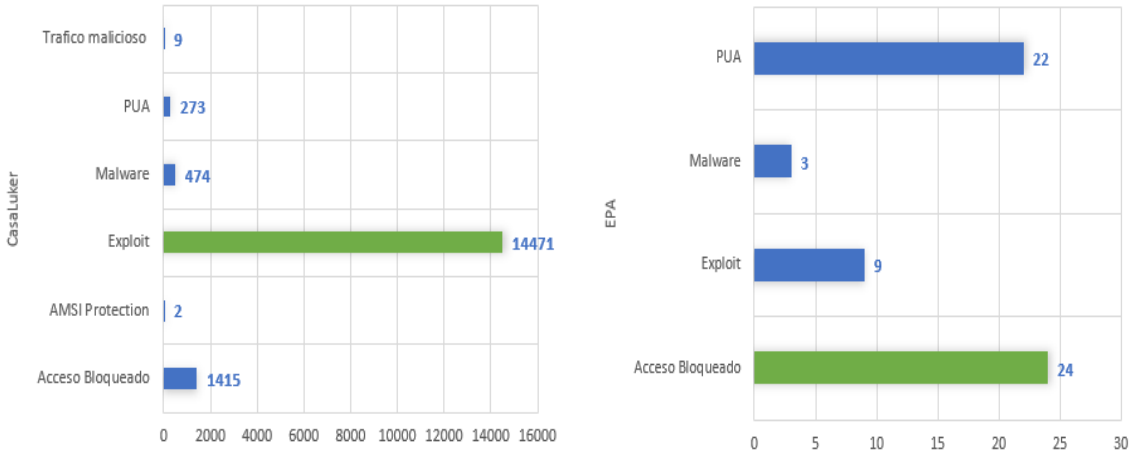
Tipo de Amenaza	Descripción
Acceso Bloqueado	Corresponde a una detección de Malware en un sitio web el cual por su contenido es bloqueado. Un ejemplo de este con base en los logs recolectados es: Access was blocked to "hangorientalauto.com" because of "Malâˆ•HTMLGen-A".
AMSI Protection	Este tipo de detecciones se obtienen bajo la aplicación Interfaz de análisis antimalware (AMSI) de Microsoft. Protege de código malicioso como scripts que se puedan ejecutar en una ventana de comando como lo puede ser PowerShell. Son mecanismos de protección permanentes.
Trafico malicioso	Este componente permite realizar una supervisión del tráfico HTTP con el propósito de detectar conexiones erróneas o con Malware.
Descarga de baja reputación	Esta aplicación permite detectar descargas con baja reputación, previamente aplica un análisis para prevenir y de ser el caso bloquear. (Sophos, 2021b)
Exploit	Este tipo de Malware es bloqueado por parte del antivirus para impedir ataques que requieran llamados a procedimientos de aplicaciones (APC) mitigando así las vulnerabilidades hacia el robo de contraseñas, registros, obtención de privilegios o el accionar de código en aplicaciones que usa la compañía

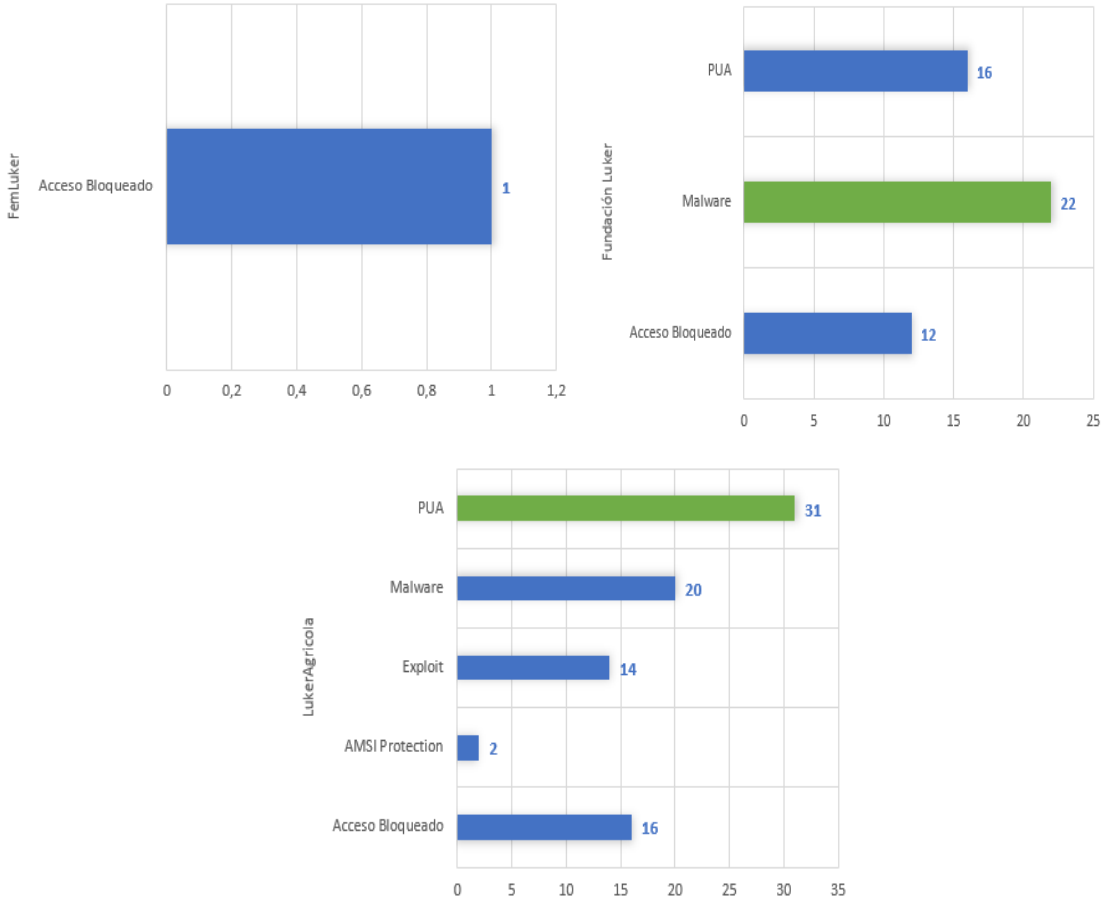
	Con base al reporte obtenido de la consola de Sophos se incluye aquí Violación APC.
Malware	Mediante esta opción se captura todas las amenazas informáticas como Toyanos, gusanos y virus
PUAs	Corresponde a las aplicaciones potencialmente no deseadas como por ejemplo adware (muestra u ofrece publicidad), marcadores, herramientas para administrar conexiónes remotas, bundleware (Programas que se instalan sin necesitarse con tan solo ejecutar una sola aplicación), descargadores, entre otros. (Sophos, 2021a)

Fuente: elaborado a partir de (Sophos Central Admin, 2021)

De esta forma, CasaLuker está con 14.471 registros catalogados como Exploit que sería la mayor amenaza, seguido de acceso bloqueados con 1415 registros. EPA por su parte, tiene 24 registros de accesos bloqueados como su mayor fuente de amenazas; Fundación Luker con 22 registros de Malware; Luker Agricola con 31 registros de PUAs y Femluker tiene tan solo una amenaza sobre accesos bloqueados como se muestra en la **Ilustración 3-13.**

Ilustración 3-13. Distribución Malware por empresa según Sophos





La consola administrativa de Sophos según los logs recolectados muestra en la **Ilustración 3-14** la severidad alta de las amenazas se encuentra en la empresa CasaLuker. La amenaza C2/generic-A fue bloqueada por el antivirus puesto que, se considera un tráfico de alto riesgo hacia una URL externa que podría propagar Malware infeccioso. La amenaza PrivGuard es un exploit que fue identificado y controlado ver **Ilustración 3-15**.

Ilustración 3-14. Severidad amenazas según Sophos

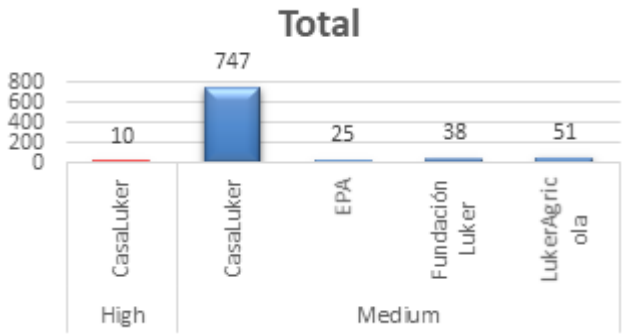
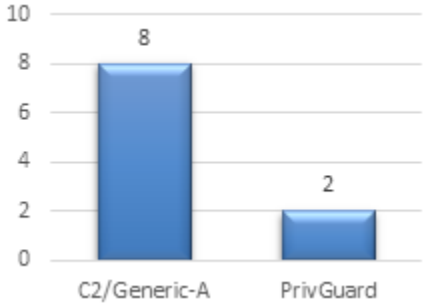


Ilustración 3-15. Distribución malware - Severidad alta



3.2 Consola seguridad Perimetral

La seguridad perimetral en una organización permite crear un muro de protección mediante un firewall que condiciona la seguridad en la red ante los diferentes ataques o vulnerabilidades externas, que se pudiesen dar en una infraestructura de comunicación. Dentro del entorno corporativo de CasaLuker, se administra un dispositivo de la familia Fortinet. Dispositivo robusto, configurable y confiable para establecer un nivel de seguridad en la red. Fortinet, pertenece a una empresa estadounidense que proporciona un gran portafolio de servicios y tecnología, una de ellas son los dispositivos y software de seguridad perimetral (Fortinet, n.d.-b).

A través de esta consola se captura todo el tráfico de la red que, condicionados bajo políticas, se define un funcionamiento que limita la navegabilidad para afianzar la estructura de seguridad de la red en la organización.

Se toman datos de 3 firewalls que se encuentran instalados en la infraestructura de red y sobre los cuales pasa todo el tráfico saliente y entrante. La información es almacenada por 2 meses en los dispositivos FortiGate y es consolidada para los respectivos informes bajo el dispositivo FortiAnalayzer que integra la información de cada uno de los firewalls.

El flujo de datos por una red es gigantesco y aprovechando la tecnología del FortiAnalayzer se extrae los logs referenciados a la seguridad con las amenazas que han sido bloqueadas. El log en la **Ilustración 3-16** muestra la fecha, la clasificación, el estado, el tipo de

amenaza, el origen entre otros, que de forma general pueden afectar el funcionamiento de la red a tal medida que sea un hueco que seguridad ante la fuga de información que se pudiese dar.

Ilustración 3-16. Registros consola Seguridad perimetral

Itime	Fecha	Hora	Dispositivo_forti	Tipo_Even	Subtype_clasificaci	Action	Ataque	Id ataque
1600147154	2020-09-15	00:16:03	FG3H0E5819902391	utm	anomaly	clear_session	udp_flood	285212772
1600147184	2020-09-15	00:16:34	FG3H0E5819902391	utm	anomaly	clear_session	udp_flood	285212772
1600147225	2020-09-15	00:17:14	FG3H0E5819902391	utm	anomaly	clear_session	udp_flood	285212772
1600147264	2020-09-15	00:17:54	FG3H0E5819902391	utm	anomaly	clear_session	udp_flood	285212772
1600147307	2020-09-15	00:18:37	FG3H0E5819902391	utm	anomaly	clear_session	udp_flood	285212772
1600147365	2020-09-15	00:19:35	FG3H0E5819902391	utm	anomaly	clear_session	udp_flood	285212772
1600147396	2020-09-15	00:20:06	FG3H0E5819902391	utm	anomaly	clear_session	udp_flood	285212772
1600147546	2020-09-15	00:22:35	FG3H0E5819902391	utm	anomaly	clear_session	udp_flood	285212772

El tipo de evento capturado mediante esta herramienta son los UTM (Unified Threat Management / Gestión Unificada de Amenazas) es la nomenclatura dada a un dispositivo de hardware o software capaz de reunir diversas funciones de seguridad como filtrado de paquetes, proxy, sistemas de detección, protección contra malware y prevención de intrusos (Fortinet, 2021d). Los ataques identificados en los logs recolectados se describen en la **Tabla 3-3**.

Tabla 3-3. Categoría amenazas según Fortinet

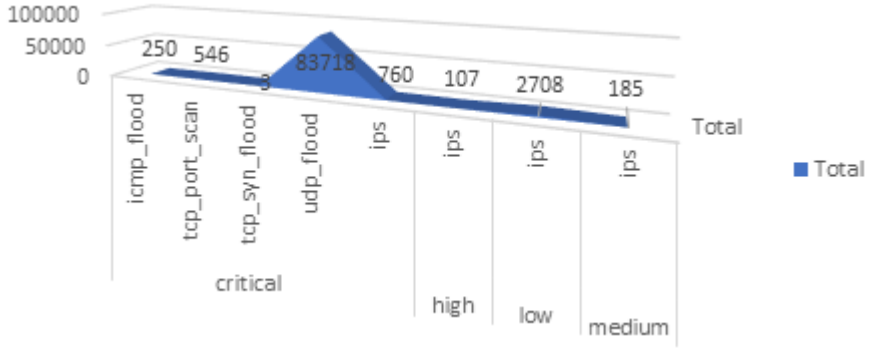
Tipo de Amenaza	Descripción
ICMP Flood	Protocolo de mensajes de control de internet (ICMP) tiene varias funciones que cuando se aplican de forma negativa pueden afectar el rendimiento de una red corporativa mediante inundación de paquetes que pueden saturar y dejar por fuera de funcionamiento un dispositivos en la red, ataques Smurt que consiste en denegaciones de servicio, ping de la muerte mediante la creación de datagramas de un mayor tamaño que el dispositivo puede soportar, entre otros (Fortinet, 2021c).
TCP port scan	Los eventos registrados en esta categoría corresponden a intentos de ataques que usen el escaneo de puertos para escuchar o interceptar algún tipo de información para uso indebido (Fortinet, 2021b).
TCP syn Food	Consiste en una falsificación de identidad para saturar la red bajo la tabla de conexiones de servidores y demás equipos que se encuentren en la infraestructura de red y provocar un colapso con el alto volumen de tránsito de paquetes (Fortinet, n.d.-a).

UDP Flood	También es conocido como ataque DoS volumétrico. Se basa en aplicar una saturación mediante el alto tránsito de datos entrantes. En general, consiste en colapsar el sistema en la que el atacante envía paquetes con una dirección IP remitente fraudulenta (Fortinet, 2021a).
IPS	Sistema de detección de intrusos, es un componente que permite bloquear la generación de eventos de Malware, rasomware entre otros ataques distribuidos mediante la red. Se consolida aquí los demás eventos detectados en la red.

Fuente: (Fortinet, 2021d)

Se recolectan 88.277 registros de los cuales, la amenaza más repetitiva es UDP flood con 83718 registros con base en la **Ilustración 3-17** y según la valoración de la herramienta es catalogado de critico puesto que, al realizarse efectivo el ataque pondría en vilo la disponibilidad los servicios ofrecidos por medio de la infraestructura de la red.

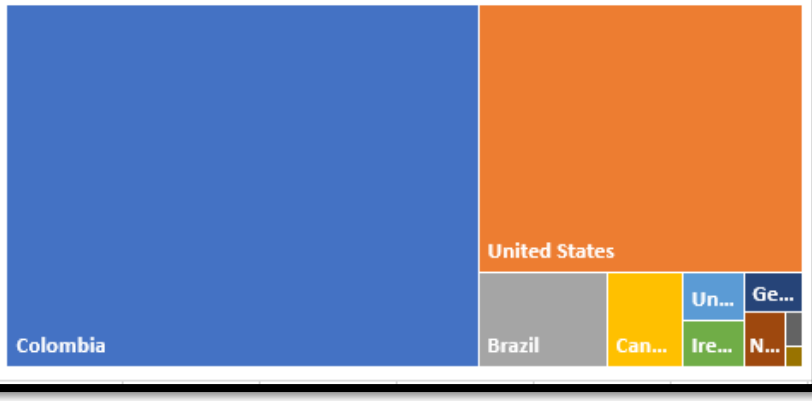
Ilustración 3-17. Distribución amenazas por severidad



En el top 10 como se visualiza en **Ilustración 3-18** de países procedentes de la amenaza la lidera Colombia, seguido de Estados unidos y Brasil.

Ilustración 3-18. Procedencia amenazas según Consola

Pais - Procedencia	Eventos
Colombia	50215
United States	25412
Brazil	3585
Canada	2116
United Kingdom	869
Ireland	840
Germany	707
Netherlands	672
China	163
France	92



3.3 Agrupación de eventos

Se agrupan los eventos de las amenazas recolectadas de cada una de las herramientas de la empresa (Office 365, Antivirus Sophos y Seguridad perimetral mediante Fortinet), para poder establecer la estructura desglose de riesgos (RBS) y proyectar la probabilidad e impacto en el desarrollo de la metodología OWASP Risk Rating.

Se toma como base la **Tabla 3-1** que tiene la clasificación de los eventos según la documentación de Microsoft y se adiciona las siguientes categorías como se visualiza en la **Tabla 3-4** para completar la unión de los logs.

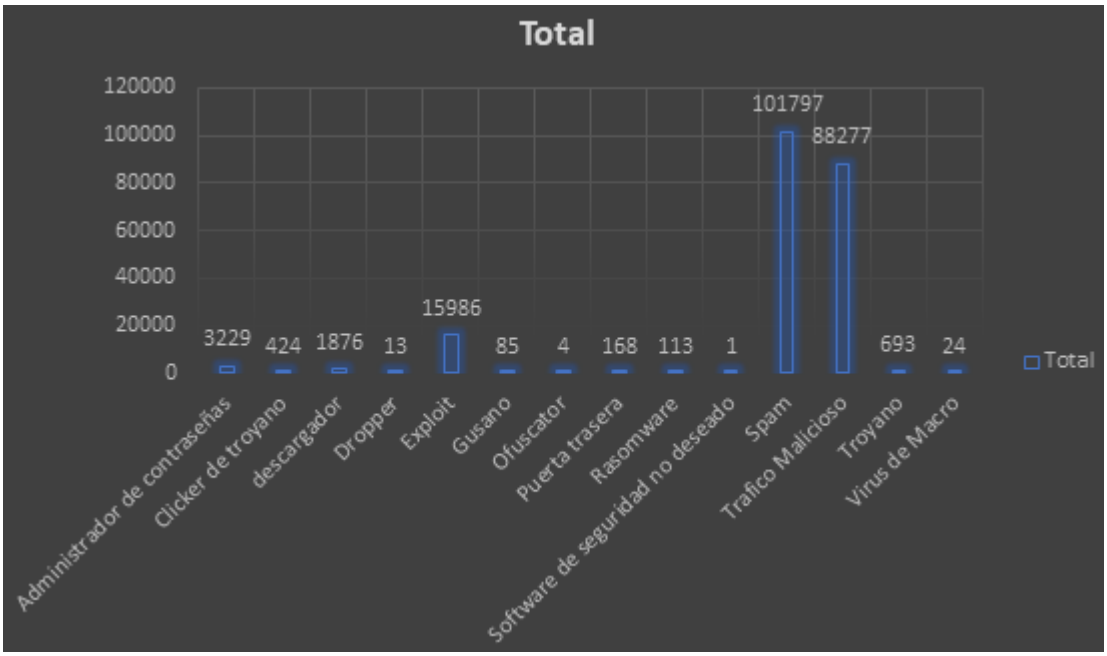
Tabla 3-4. Complemento categorías de amenazas

Tipo de Amenaza	Descripción
Spam	Correos de dudosa procedencia o con contenido maliciosos que son identificados por la plataforma de Microsoft
Trafico Malicioso	Consiste en el tránsito de paquetes por medio de una infraestructura red donde el sistema de seguridad perimetral identifica como una amenaza, por el comportamiento que este genera en el desempeño y rendimiento en la transmisión de datos.

Fuente: (Fortinet, 2021d) y (Microsoft, 2021d)

La **Ilustración 3-19** contiene 212.690 registros donde se consolidan las amenazas de los (Logs) que se generaron en el intervalo de tiempo estudiado.

Ilustración 3-19. Distribución de amenazas por categoría



Capítulo 4. Propuesta metodológica marco gestión de riesgo basado en análisis de datos de seguridad

Considerando el entorno, la metodología OWAPS y los registros (Logs) de las herramientas tecnológicas que puede tener una organización, se establece las siguientes fases como se visualizan en la **Ilustración 4-1** para la Gestión de Riesgos de Tecnologías de la Información y Comunicación con énfasis en ambientes multi empresariales.

Ilustración 4-1. Fases de la propuesta del Marco Metodológico

4.1 Fase 1: Inventario de recursos tecnológicos de la empresa

Tener un conocimiento claro del funcionamiento del negocio es clave en la gestión del riesgo, puesto que permite identificar las debilidades del sistema en cada uno de los vagones del proceso organizativo, en el cumplimiento de los objetivos corporativos (MinTIC, 2016). Esta fase se enfoca en saber que recursos tecnológicos cuenta la organización, la cual se puede apreciar en la **Tabla 4-1** en la que clasifica según el autor (Valencia et al., 2016b) bajo conceptos de capas de Tecnologías de la Información y Comunicaciones.

Tabla 4-1. Inventario Recursos Tecnológicos

#	Capa	Descripción
1	Proceso de negocio	En el cumplimiento de los objetivos son las actividades propias de la organización como motor de operación (mapa de procesos).
2	Servicios de TI	Estos servicios se pueden componer de infraestructura tecnológica, procesos y operación para prestar beneficio a los usuarios de la organización. Un ejemplo de ello sería correo electrónico o herramienta de colaboración como chat (Microsoft Teams).
3	Datos – Información – Conocimiento	Dada la importancia para la empresa está capa requieren de mayor atención puesto que es el modelo de negocio en su pasado, presente y futuro
4	Sistemas de información Transaccionales	Corresponde a la aplicaciones o sistemas de información en las que facilita a la organización la ejecución de sus procesos. Por ejemplo, un Enterprise Resource Planning (ERP) como lo es System Applications and Products (SAP), Aplicativos para gestión de nómina, Gestión documental entre otros.
5	Sistemas de información soporte	Consiste en las herramientas de software que permite apoyar el negocio en diferentes actividades como por ejemplo el Office 365 de Microsoft, antivirus, software utilitario y demás programas que no ampara un proceso especial por parte de la organización.
6	Motores de Bases de datos	Estas herramientas regularmente se le conocen como gestores de bases de datos con las que permite administrar los datos que tiene una organización mediante una aplicación o sistema de información. Entre los motores de base de datos más comunes se encuentra el Oracle, SQL Server, MySQL, PosgretSQL, SQlite
7	Sistemas operativos	Corresponde al programa que controla los procesos de un Hardware como un computador, un teléfono móvil, un servidor, una radiofrecuencia ente otros; que a su vez permite la ejecución de otras aplicaciones. Los sistemas operativos más comunes que se puede referencia son Windows, Linux, macOS, Android, Unix.
8	Pc's escritorio e impresoras	Estos dispositivos informáticos permiten procesar información, acceder a recursos como sistemas de información en una red o trabajos locales. Son equipos de cómputo del trabajo diario

		de los usuarios en los puestos activos de trabajo en la organización.
9	Servidores (Físicos, Virtuales y en la nube)	Estos dispositivos ejercen una operativiblidad alta para la ejecución de tareas específicas, por la que requiere de amplias características técnicas previamente diseñadas y acondicionadas para la labor correspondiente. Un ejemplo de estos equipos son los servidores de dominio, de impresoras, Base de datos, de aplicaciones entre otros. Estos pueden ser servidores físicos, virtuales (varios servidores dentro de uno físico) o servidores que se encuentra en la nube.
10	Centro de redes y cableado	Consiste en la infraestructura de red que tiene la organización con la cual se puede establecer la unión de dispositivos que depende de este medio mediante un cableado estructurado y demás tecnología que permita la interconexión
11	Centro de computo	Es un espacio o sitio definido para la ubicación de dispositivos que procesan información, equipos que establecen comunicación o almacenamiento de información. son dispositivos críticos y de cuidado.
12	Energía	Un ejemplo de este nivel corresponde a un sistema de alimentación ininterrumpida (UPS) que permiten almacenar y proteger equipos o circuitos de red eléctrica regulada para los equipos que dependen de un funcionamiento constante que al interrumpirse afecta la operación de la compañía

Fuente: elaborado a partir de (Valencia et al., 2016b)

El inventario de recursos tecnológicos se debe consolidar con los responsables del servicio (área de Tecnología de la Información o afines) y actores propios del negocio. Con este insumo se podrá ofrecer una visual de la infraestructura de la compañía, responsables o áreas que depende de estos y evaluar sobre que herramientas puedo obtener registros (Logs) que permitan tabular comportamientos e información sobre las vulnerabilidades y/o amenazas del entorno, para estimar un grado de prioridad e impacto en la determinación de la gravedad del riesgo. La **Tabla 4-2** contiene los elementos de cada capa del entorno multi empresarial de CasaLuker. Los logs se recolectan de la capa de Sistemas de Información Soporte donde está la consola administrativa de office 365 y antivirus Sophos; y de la capa 10 centro de redes y cableado por medio del Firewall Fortinet.

Tabla 4-2. Distribución de activos según capas tecnológicas

#	Capa	Descripción
12	Energía	27 UPS (Sistema de alimentación ininterrumpida)
11	Centro Computo	- Un Data center en sede propia - Un Data center tercerizado con proveedor IBM
10	Centro de redes y cableado	- 80 switch - 4 firewall - 150 dispositivos para proporcionar Inalámbrica - Cableado estructurado en las 22 sedes - 19 enlace de datos dedicados - 11 bandas anchas
9	Servidores (Físicos, Virtuales y en la nube)	4 servidores físicos (Aplicación contable Agrowin – Nomina – servidores para soportar los servidores virtuales) 26 servidores virtuales, algunos de estos son para (Controlador de dominio – Monitoreo de red – mesa de servicio – manejo de cubos – Impresión – Docuware – Sincronizacion directorio activo – replicador – Base de datos – Daruma – entre otros) 1 NAS para almacenamiento
8	Pc's escritorio e impresoras	Equipos computo (Computadores usuarios finales): - CasaLuker (830) - Fundacion Luker (45) - Luker Agricola (58) - Femluker (8) - EPA (30) Impresoras: - CasaLuker (98) - Fundacion Luker (2) - Luker Agricola (3) - Femluker (2) - EPA (1)
7	Sistemas operativos	En servidores físicos y virtuales: - Windows Server 2016 STD - Windows Server 2008 R2 STD - Windows Server 2012 R2 STD - Windows Server 2019 STD

		NAS: - Windows Storage Server 2012 En equipos computo: - Windows 10 Profesional - MacOS Catalina
6	Motores de Bases de datos	Oracle SQL Hana
5	Sistemas de información soporte	- Software ofimático (suite Office 365) - Antivirus (Sophos) - Software Backup - Forticlient (VPN) - SAP GUI for Windows - Navegador (Google Chrome o Microsoft Edge) - Software utilitario (Adobe acrobat) - Snow Inventory - Software específico para cada empresa como (OPA - Ordenamientos Profesionales Automatizados, Suite de adobe cloud, Minitab, Statgraphics, articulate, TOAD, Genesis, Forecastpro, Autocad, Power BI, Agrowin, otros)
4	Sistemas de información Transaccionales	Enterprise Resource Planning (ERP): - SAP Nomina: - Queryx 7 Gestión casos: - Helppeople Manejo fondo empleados: - OPA Gestión documental - Daruma ERP: Agrowin

3	Datos – Información – Conocimiento	La información es categorizada según los procesos de la compañía. De forma general información sobre producción, financiera, logística, comercial, talento, investigación, nominal, proyectos de inversión entre otros.
2	Servicios de TI	Comunicaciones: - Internet - Canales de datos - Red cableada - Red Inalámbrica - Conexión VPN - Telefonía Colaborativos: - Correo Electrónico - Intranet - Mensajería instantánea - Videoconferencia Seguridad Perimetral: - Firewall Hardware: - Equipos computo (portátiles – equipos escritorio) - Servidores - Equipos Radiofrecuencias - UPS - Impresoras Ofimática: - Suite office 365 - Antivirus - Aplicativo Backup usuarios - Aplicativo impresión facturas - Sistemas operativos - Software Utilitario Sistemas de información: - SAP en sus entornos de pruebas – Calidad - Productivo

		- Nomina - Servicios adicionales office 365 como sharepoint - Directorio Activo - Sistema inventario de equipos computo - Sistema monitoreo de red Mesa de servicio: - Técnico - Funcional Base de datos: - Oracle - SQL Almacenamiento: - Almacenamiento en NAS
1	Proceso de negocio	CasaLuker: Empresa de consumo masivo que tiene una definición interna de negocios para potencializar la eficiencia de sus procesos Macroproceso: Comercializar productos de consumo masivo. Cultivar – Producir – comercializar – Distribuir – recaudar. Fundación Luker: Organización privada sin ánimo de lucro para apoyo social en temas de educación. Macroproceso: Generar proyectos de educación. Luker Agricola: Es una empresa dedicada al cultivo agrícola. Macroproceso: Cultivar palma de aceite y frutos oleaginosos. Adicional cultivar el cacao FemLuker: Organización de economía solidaria sin ánimo de lucro para beneficio de los colaboradores del entorno multi empresarial Macroproceso: Contribuir al desarrollo integral del asociado mediante la prestación de servicios financieros y de bienestar EPA:

		Empresa panameña de consumo masivo. En el entorno corporativo hay una sección de colaborares que prestan servicios a la operación de esta. Macroproceso: Comercializar productos de consumo masivo

4.2 Fase 2: Identificación del Riesgo

Está fase establecerá los eventos que pueden generarse en el entorno corporativo. Por tanto, se toma de referencia las herramientas tecnológicas instaladas en las empresas para obtener registros sobre vulnerabilidades, posibles ataques y/o amenazas que se convierten en un suministro del presente proceso para construir el escenario de riesgo sobre esas falencias y comportamientos. De esta forma, uno de los pasos de esta fase es consolidar los registros (Logs) para visualizar un precedente, seguido de un análisis de los activos y servicios esenciales para que la empresa opere (Munir et al., 2015). Esta labor debe integrar actores como los integrantes de Tecnologia de la información y colaboradores con conocimiento de la ejecución de procesos.

4.3 Categorización de amenazas

Para la identificación del riesgo se usó una herramienta jerárquica que se llama estructura de desglose de riesgos (RBS) con el propósito de organizar las amenazas en categorías que fueron referenciadas con la documentación de Microsoft para una adecuada estandarización y gestión (López et al., 2014). Por tanto, la **Tabla 4-3** contiene una categorización de las amenazas, su descripción y cantidad de ocurrencias encontradas en las herramientas tecnológicas del entorno multi empresarial.

Tabla 4-3. Categorización amenazas entorno multi empresarial

#	Categoría de amenaza	Descripción categoría	Cuantas tipologías – Ver (**Anexo A**)	Número de ocurrencias
1	Inadecuada gestión de contraseñas	Esta amenaza recopila datos del usuario como contraseñas de acceso y la cuenta de ingreso, que por lo general se realiza mediante un registro de las	4 tipos	982

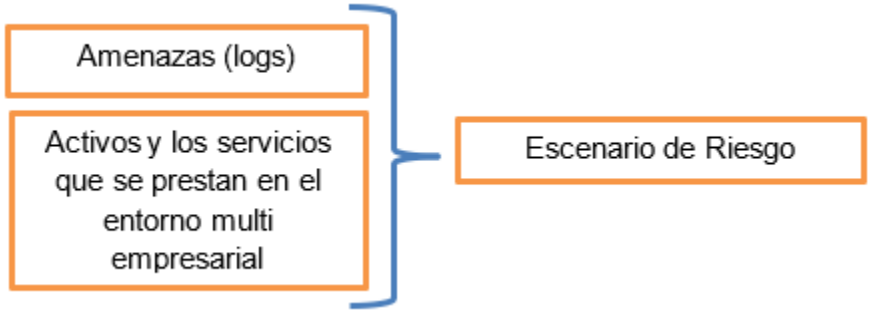
		pulsaciones del teclado o por medio de correos que tienen finalidad de aprovechar la inocencia de los usuarios y captura datos sensibles para luego suplantar la identidad (Microsoft, 2021b).		
2	Clicker de troyano	Este tipo de amenaza genera accesos de forma automática en los anuncios o publicidad dada en los sitios web, de tal forma que pueden generar instalaciones no deseadas en el equipo computo (Microsoft, 2021b).	84 tipos	424
3	Descargador	Esta amenaza genera una descarga de otro malware en el equipo computo. Una condición de este tipo de amenaza es la necesidad de que esté conectado al internet (Microsoft, 2021b).	19 tipos	1876
4	Dropper	A contrario de la amenaza descargador, Dropper no requiere de internet. Su fin es instalar archivos maliciosos en el equipo computo (Microsoft, 2021b).	1 tipo	13
5	Exploit	Las vulnerabilidades que puede tener una aplicación son usabas por este tipo de amenaza, alterando propiedades del código con el cual, él atacante pueda obtener acceso al dispositivo y de tal forma pueda ejecutar tareas mucho más específicas y elaboradas (Microsoft, 2021b).	14 tipos	15986
6	Gusano	Este tipo de amenaza se propaga fácilmente aprovechando la vulnerabilidad de un software por medio de correo electrónico, archivos compartidos por medio de la red o aplicaciones, redes sociales, mensajería instantánea como lo podría ser un Microsoft Teams, unidades extraíbles como las memorias USB entre otros (Microsoft, 2021b).	2 tipos	85
7	Ofuscator	Esta amenaza se camufla lo que complica la eliminación de este en un sistema, a un más cuando ni se sabe cuál es el propósito de su ataque en el dispositivo (Microsoft, 2021b).	1 tipo	4
8	Puerta trasera	Proporciona acceso remoto y control de un equipo de cómputo a personas con conocimiento en programación para ejecutar acciones maliciosas (Hackers) (Microsoft, 2021b).	3 tipos	168

9	Rasomware	Esta amenaza se ha vuelto muy común, Cifra o modifica los archivos para que no puedan ser usados por el usuario. La mayor parte de este tipo de ataques son extorsivos para que el usuario pague y pueda recuperar la información (Microsoft, 2021b).	14 tipos	113
10	Software de seguridad no deseado	Su fin es mostrar alertas de amenazas que quizás ni existan en el dispositivo. Actúa como un antivirus o programa de protección, pero no lo es. Por lo regular se instala ocultamente dentro de otro software que luego se activa para la generación de avisos (Microsoft, 2021b)..	1 tipo	1
11	Spam	Esta amenaza corresponde a correos electrónicos confusos, de dudosa procedencia que, por lo general, tiene contenido malicioso para desplegar en el equipo de cómputo otras amenazas. Son identificados por la plataforma de correo que en este caso es Microsoft (Microsoft, 2021a).	11864 tipo según su procedencia	100994
12	Trafico Malicioso	Está amenaza consiste en un tráfico excesivo de paquetes por medio de una infraestructura de red que mediante un sistema de seguridad es identificado como maliciosos. El comportamiento de este es causar lentitud en el tráfico de paquete que realmente son buenos, baja el desempeño y puede generar daños en dispositivos de red al igual de transmitir otro tipo de amenazas a los equipos computo.(Fortinet, 2021b)	69 tipos	88277
13	Troyano	Como su nombre lo indica, usa un tipo de camuflaje para parecer inofensivo. Una vez son descargados e instalados comienzan aplicar su propósito de robar información personal, dar acceso a los atacantes o descargar otros Malware (Microsoft, 2021a).	28 tipos	693
14	Virus de Macro	Por lo general, este tipo de amenaza se propaga por medio de documentos (suite de office 365) que han sido infectados que se activan al momento de abrirlos (Microsoft, 2021a).	1 tipo	24

4.3.1 Escenario de riesgo

Como se observa en la **Ilustración 4-2**, se realiza una agrupación de datos de las amenazas detectadas (Logs) del entorno multi empresarial como se categorizó en el anterior paso, que cruzados con el inventario de activos establecidos en la fase de Inventario de recursos tecnológicos de la empresa se obtiene el escenario de riesgo para establecer el respectivo análisis.

Ilustración 4-2. Escenario de Riesgo



El escenario de riesgo se establece mediante la metodología de Jerry FitzGerald similar al proceso realizado por el autor (Edgard Pujaico Paredes, 2018) que permite cruzar las amenazas con los activos tecnológicos que la empresa considere son de importancia para su operación. Teniendo en cuenta el entorno Multi empresarial y de forma general se obtienen 95 escenarios de riesgos que se consolidan en el (**Anexo B**).

4.4 Fase 3: Determinación de la gravedad del Riesgo

Esta fase combina la estimación de la probabilidad e impacto de tal forma que se establecen los criterios para evaluar cada escenario de riesgo.

4.4.1 Probabilidad

Considerando los factores de agente de amenaza y de vulnerabilidad se procederá a calcular la probabilidad de ocurrencia a partir de la **Ilustración 4-3**.

Ilustración 4-3. Cálculo probabilidad

$$P = \frac{\sum FA + \sum FV}{n}$$

Fuente: elaborado a partir de (Williams, n.d.)

Se toman por defecto los criterios de evaluación de Nivel de habilidad, Motivación y Oportunidad como se visualizan en **Ilustración 2-2** de los factores de agente de amenaza. Para el concepto del tamaño se toman en cuenta los registros (Logs) recolectados de las herramientas tecnológicas de la empresa para definir el volumen de incidencia, determinando los criterios establecidos en **Tabla 4-4** para obtener una calificación y ser computada.

Tabla 4-4. Calificación criterio tamaño en los factores de amenaza

Valor	Descripción cuantitativa	Descripción cualitativa
0	Entre 0 y 1 evento	Poca probabilidad de ocurrencia en los últimos seis meses
1	Entre 2 a 100 eventos	Se ha presentado entre dos y cien ocurrencias en los últimos seis meses
2	Entre 101 a 1000 eventos	Se ha presentado entre ciento y uno y mil ocurrencias en los últimos seis meses
3	Entre 1.001 a 5.000 eventos	Se ha presentado entre mil y uno y cinco mil ocurrencias en los últimos seis meses
4	Entre 5.001 a 10.000 eventos	Se ha presentado entre cinco mil y uno y diez mil ocurrencias en los últimos seis meses
5	Entre 10001 a 30.000 eventos	Se ha presentado entre diez mil y uno y treinta mil ocurrencias en los últimos seis meses
6	Entre 30.001 a 50.000 eventos	Se ha presentado entre treinta mil y uno y cincuenta mil ocurrencias en los últimos seis meses
7	Entre 50.001 a 80.000 eventos	Se ha presentado entre cincuenta mil y uno y ochenta mil ocurrencias en los últimos seis meses
8	Entre 80.001 a 100.000 eventos	Se ha presentado entre ochenta mil y uno y cien mil ocurrencias en los últimos seis meses
9	Mayor a 100.000 eventos	Se ha presentado más de cien mil ocurrencias

Fuente: Análisis de logs realizados al interior del entorno multi empresarial de CasaLuker en un periodo de seis meses.

De esta forma, la **Ilustración 4-4** contiene los criterios definidos para aplicar la evaluación correspondiente.

Ilustración 4-4. Factores de Agente de Amenaza

Factores de agentes de amenaza			
Nivel de Habilidad	**Motivación**	**Oportunidad**	**Tamaño**
0-	0-	0- Se requiere acceso total o recursos costosos	0- Entre 0 y 1 evento
1- Sin habilidades técnicas	1- Recompensa baja o nula	1-	1- Entre 2 a 100 eventos
2-	2-	2-	2- Entre 101 a 1000 eventos
3- Algunas habilidades técnicas	3-	3-	3- Entre 1.001 a 5.000 eventos
4-	4- Recompensa posible	4- Se requiere acceso o recursos especiales	4- Entre 5.001 a 10.000 eventos
5- Usuario avanzado en computadores	5-	5-	5- Entre 10001 a 30.000 eventos
6- Habilidades de programación y redes	6-	6-	6- Entre 30.001 a 50.000 eventos
7-	7-	7- Se requiere algún acceso o recursos	7- Entre 50.001 a 80.000 eventos
8-	8-	8-	8- Entre 80.001 a 100.000 eventos
9- Habilidades de penetración de	9- Recompensa alta	9- No se requiere acceso o recursos	9- Mayor a 100.000 eventos

Fuente: elaborado a partir de (Williams, n.d.)

Ahora, el siguiente paso es calificar los factores de vulnerabilidad con base en **Ilustración 2-3** tomando los conceptos por defecto de facilidad de explotación y detección de intrusiones, este último se tiene en cuenta con los registros obtenidos de las amenazas como una calificación en detección activa con las herramientas existentes. Adicional, se personaliza el criterio de facilidad de descubrimiento en la que se especula que tan breve es para el atacante poder reconocer una deficiencia en la seguridad que pueda tener una compañía como se visualiza en la **Tabla 4-5** teniendo en cuenta los registros (logs)

recolectados de las herramientas existentes sobre las amenazas detectadas del entorno multi empresarial.

Tabla 4-5. Calificación criterio facilidad de descubrimiento

Valor	Descripción cuantitativa	Descripción cualitativa
1	Entre 1 a 10 eventos	Vulnerabilidad baja si el número de ocurrencias esta entre 1 y 10 en los últimos seis meses. (Prácticamente imposible).
3	Entre 11 a 1.000 eventos	Vulnerabilidad media si el número de ocurrencias esta entre 11 y 1.000 en los últimos seis meses. (Difícil)
6	Entre 1.001 a 10.000 eventos	Vulnerabilidad alta si el número de ocurrencias esta entre 1.001 y 10.000 en los últimos seis meses. (Fácil)
9	Mayor a 10.000 eventos	Vulnerabilidad muy alta si el número de ocurrencias es mayor a 10.000 (Muy fácil)

Fuente: Análisis de logs realizados al interior del entorno multi empresarial de CasaLuker en un periodo de seis meses.

De esta manera, la **Ilustración 4-5** contiene los criterios definidos para aplicar la evaluación correspondiente.

Ilustración 4-5. Factores de vulnerabilidad

Factores de vulnerabilidad			
Facilidad de descubrimiento	**Facilidad de explotación**	**Conciencia**	**Detección de Intrusiones**
0-	0-	0-	0-
1- Entre 1 a 10 eventos	1- Teórico	1- Desconocido	1- Registrada y revisada
2-	2-	2-	2-
3- Entre 11 a 1.000 eventos	3- Difícil	3-	3- Detección activa con las herramientas existentes
4-	4-	4- Oculto	4-
5-	5- Fácil	5-	5-
6- Entre 1.001 a 10.000 eventos	6-	6- Obvio	6-
7-	7-	7-	7-
8-	8-	8-	8- Registrada sin revisión
9- Mayor a 10.000 eventos	9- Herramientas automatizadas disponibles	9- Conocimiento público	9- No registrada

Fuente: elaborado a partir de (Williams, n.d.)

4.4.2 Impacto

El impacto hace referencia a las consecuencias al hacerse efectivo un riesgo para lo cual, se procederá a calcular el impacto a partir de la **Ilustración 4-6**.

Ilustración 4-6. Cálculo de impacto

$$I = \frac{\sum IT + \sum IC}{n}$$

Fuente: elaborado a partir de (Williams, n.d.)

Se toman por defecto los criterios de evaluación de impacto técnico como lo es la pérdida de confidencialidad, de integridad, de disponibilidad y responsabilidad como se visualizan en la **Ilustración 2-4**. El impacto comercial también se toman los criterios por defectos estipulados en la **Ilustración 2-5**.

4.4.3 Gravedad del Riesgo

Se establece la descripción de los conceptos del nivel de riesgo también conocido como el nivel de aceptación o apetito del riesgo visualizados en la **Tabla 4-6** para realizar el cruce de la probabilidad e impacto como se aprecia en la **Ilustración 2-6** y determinar en qué posición se encuentra el escenario de riesgo. El resultado de este proceso se convierte en el insumo para evaluar los controles existentes y ver las posibles mejoras que se le puedan aplicar.

Tabla 4-6. Nivel del Riesgo

Métrica	Nivel del riesgo	Descripción
Entre 0 y < 3	Bajo	El riesgo es detectable con facilidad, las medidas de control que se encuentra vigentes están mitigando los eventos de ocurrencia. Se sugiere estar atento a la actualización de medidas conforme avanza la tecnología.
Entre 3 y < 6	Medio	El riesgo es moderado, se deben evaluar los mecanismos actuales de control para reducir su probabilidad de ocurrencia y en caso de presentarse, su impacto.

Entre 6 y < 9	Alto o Critico	El riesgo detectado es muy alto y posiblemente los controles actuales son insuficientes para mitigar la ocurrencia. Se sugiere implementar nuevas medidas de contención y control.

Fuente: elaborado a partir de (Williams, n.d.)

La matriz construida con los parámetros mencionados se encuentra en el (**Anexo C**).

4.4.4 Controles

Al existir cualquier tipo de riesgo que limite las operaciones de la compañía y pongan en vilo la seguridad de la información, se deben aplicar controles que disminuyan ese riesgo, que sea aceptable, que de tranquilidad de que cada proceso realizado por la compañía para el cumplimiento de sus objetivos organizativos. Los controles de seguridad de la información con base ISO/IEC 27001, se construyen bajo combinación de procedimientos, tecnología que quizás la empresa ya tenga o deba invertir y los usuarios referentes quienes tienen el conocimiento de cómo opera la compañía (Valencia Duque, 2021). Muchos de estos controles deben ser valorados según criterios de costo por si deben implementar aplicativos o tecnología y estos deben ser comparados con el beneficio que puede darse para compañía, ya que pueden estar sometidos restricciones de tipo cultural cuando implica cambiar la forma de hacer las actividades o el entorno operativo al aumentar algún paso adicional a los que actualmente tiene.

CasaLuker usa algunos conceptos de la ISO 27002 basados en 114 controles de Tecnología de la Información los cuales están enfocados hacia la continuidad del negocio en términos de operación y seguridad de la información que se describen a continuación:

- Cuenta con un equipo de seguridad perimetral (Firewall) para evitar el acceso no autorizado.
- Las modificaciones en las configuraciones de los equipos están restringidas al usuario administrador.
- Perfiles de usuarios para el acceso a la información.
- Copias de seguridad de los aplicativos.

- Antivirus en todos los equipos computo (Pcs escritorio y portátiles) de usuarios finales.
- Control de puertos USB a través de políticas del End-Point mediante el antivirus.
- Control de instalación de aplicaciones a través de políticas de grupo del directorio activo.
- El acceso a Internet está restringido para la mayoría de los usuarios para evitar el ingreso a paginas maliciosas o descarga de archivos.
- Copias de seguridad de las bases de datos manejadas en los servidores.
- Equipos de comunicación de respaldo.
- Esquemas de copia de seguridad de los servidores
- Servidor de respaldo
- Esquemas de copia de seguridad de los usuarios finales considerados críticos por sus cargos desempeñados en la organización.
- Monitoreo de servidores y enlaces considerados críticos para las operaciones de la compañía mediante alertas tempranas.
- Contrato con proveedor de comunicaciones con ANS del 98,6%. Para garantizar la conectividad y soportado bajo una mesa de servicio con atención 7x24.
- Enlaces de comunicaciones de contingencias en sedes y aplicativos críticos para la operación de la compañía.
- Esquema para renovar periódicamente los equipos computo (Pcs escritorio y portátiles) de usuarios finales.
- Actualización periódica de los aplicativos a las últimas versiones.
- Datacenter tercerizado para manejo del ERP con servicio 7x24 con soporte de primer nivel y escalamiento cuando sea requerido.

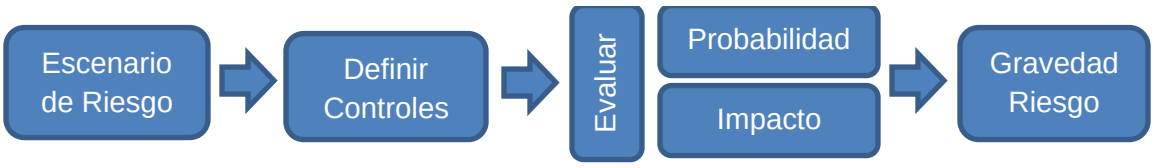
Los controles mencionados aplican al contexto multi empresarial puesto que dependen de área de Tecnología de la Información. por tanto, este paso consiste en validar los controles existentes para la mitigación de los escenarios de riesgo identificados con severidad alta según la **Tabla 2-2**.

4.4.5 Riesgo Residual

El Riesgo Residual consiste en verificar el riesgo que queda al aplicar los controles que la empresa tenga vigentes, como los referenciados en el anterior punto (Valencia Duque, 2018). Por tanto, se evalúa el efecto que producen esos controles sobre el escenario de riesgo como se visualiza en la **Ilustración 4-7**. La implementación de controles altera el comportamiento del Riesgo Residual con un simple propósito el cual es, obtener un nivel aceptado de riesgo y con la obligación de estar realizando actualizaciones periódicas para verificar si este sigue prestando el mismo cumplimiento o deba ser replanteado con nuevos procesos, tecnología, entre otros.

Considerando el proceso establecido mediante la metodología OWASP Risk Rating se realiza nuevamente la evaluación sobre los conceptos establecidos en la probabilidad e impacto para obtener nuevamente la Gravedad del Riesgo.

Ilustración 4-7. Evaluación del Riesgo Pos-controles



4.5 Fase 4: Determinar que arreglar

Una vez se ha identificado como están calificados los escenarios de riesgos, aun con los controles vigentes se puede establecer un plan de manejo de riesgos, que consiste en una serie de actividades que mejore cada vez la barrera ante incidentes. Esta panorámica permite a los dirigentes trazar una ruta de trabajo y ver como en el futuro se va visualizando un comportamiento que aporte a la confidencialidad, integridad y disponibilidad de la información. De esta forma, se toman algunos conceptos ISO/IEC 27005 como los estipulados por el autor (Valencia Duque, 2021) y que se estructura en la **Tabla 4-7** donde se toma el Escenario de Riesgo identificado en la fase 1, la calificación que obtuvo al implementar los controles seguido de una estrategia para tratar ese riesgo que se establece en la **Tabla 4-8** con base en los conceptos referenciado por la (ISO 31000,

2018). También se adiciona los nuevos controles y señalando él o los responsables de la ejecución en un tiempo determinado. Por último, un seguimiento del proceso indicando el estado actual, las observaciones que se tienen de la gestión y el costo estimado que implicaría ese control.

Tabla 4-7. Plan Tratamiento Riesgos

#	Escenario de Riesgo	Severidad del Riesgo al implementar el control	Estrategia de Tratamiento	Control - actividad a desarrollar	Responsable	Fecha cierre	Seguimiento		Costo Aprox. Invesión
							Estado	Observaciones	

Fuente: Elaborado a partir de (Valencia Duque, 2021)

Tabla 4-8. Estrategias tratamiento de riesgo

Estrategia	Descripción
Aceptación del riesgo	Corresponde a una decisión de la organización de aceptar las consecuencias sin aplicar acciones de mitigación.
Transferencia del riesgo	Consiste en ceder la responsabilidad a una persona o ente organizativo con capacidades para que realice la labor de prevenir, eliminar o asumir el costo financiero dado el caso de que el evento adverso ocurra.
Mitigación del riesgo	Permite el desarrollo o ejecución de acciones para reducir el impacto negativo o la probabilidad de ocurrencia

Fuente: Elaborado a partir de (ISO 31000, 2018)

Capítulo 5. Validación del marco de gestión de riesgos de Tecnologías de la Información y Comunicación

Se selecciona una de las empresas del entorno multi empresarial y se aplica las fases de la propuesta como se establece en la **Ilustración 4-1**. La empresa seleccionada es Femluker (Fondo de empleados de CasaLuker) que se encuentra ubicada en dos sedes del entorno multi empresarial y que adopta las prácticas de Tecnología de la Información de CasaLuker. La toma de registros (logs) se aplica sobre las herramientas descritas del presente documento en la que se evidencian las amenazas o eventos detectados y se adaptan a algunos conceptos expuestos en el top diez de OWASP como el control de acceso, exposición de datos confidenciales e inyección a nivel de captura de datos sensibles (OWASP, 2021) sobre las categorías obtenidas en la consolidación de logs, que pudiesen aprovechar los atacantes para obtener algún tipo de información. Considerando las restricciones de la empresa y del entorno multi empresarial no se tiene acceso a los logs que pueden ofrecer las bases de datos de las que depende la empresa FemLuker

5.1 Fase1: Inventario de Recursos Tecnológicos de la empresa Femluker

La **Tabla 5-1** contiene la relación de los activos y servicios de la empresa

Tabla 5-1. Inventario de Recursos Tecnológicos de la Empresa FemLuker

#	Capa	Descripción
12	Energía	2 UPS (Sistema de Alimentación Ininterrumpida)

11	Centro Computo	- Un Data center en sede propia
10	Centro de redes y cableado	- 2 switch - 1 firewall - 2 dispositivos para proporcionar Inalámbrica - Cableado estructurado en las 2 sedes - 2 enlace de datos dedicados
9	Servidores (Físicos, Virtuales y en la nube)	1 servidor físico para ERP de Ordenamientos Profesionales Automatizados (OPA) 1 servidores virtuales para manejo de base de datos
8	Pc's escritorio e impresoras	8 equipos computo (Computadores usuarios finales) 2 impresoras
7	Sistemas operativos	En servidor físico y virtual: - Windows Server 2019 STD En equipos computo: - Windows 10 Profesional
6	Motores de Bases de datos	SQL
5	Sistemas de información soporte	- Software ofimático (suite Office 365) - Antivirus (Sophos) - Forticlient (VPN) - Navegador (Google Chrome o Microsoft Edge) - Software utilitario (Adobe acrobat) - Snow Inventory
4	Sistemas de Información Transaccionales	Enterprise Resource Planning (ERP): - Ordenamientos Profesionales Automatizados (OPA) para la administración del fondo empleados Nomina: - Queryx 7 Gestión casos: - Helppeople Manejo fondo empleados: - OPA

3	Datos – Información – Conocimiento	La información es categorizada según los procesos de la compañía. De forma general información nominal de los usuarios finales pertenecientes al fondo de empleados.
2	Servicios de TI	Comunicaciones: - Internet - Canales de datos - Red cableada - Red Inalámbrica - Conexión VPN - Telefonía Colaborativos: - Correo Electrónico - Intranet - Mensajería instantánea - Videoconferencia Seguridad Perimetral: - Firewall Hardware: - Equipos computo (portátiles – equipos escritorio) - Servidores - UPS - Impresoras Ofimática: - Suite office 365 - Antivirus - Sistemas operativos - Software Utilitario Sistemas de información: - Nomina - Servicios adicionales office 365 como sharepoint - Directorio Activo - Sistema monitoreo de red

		Mesa de servicio: - Técnico - Funcional Base de datos: - SQL
1	Proceso de negocio	FemLuker: Se describe como una organización de economía solidaria sin ánimo de lucro para beneficio de los colaboradores del entorno multi empresarial Macroproceso: Contribuir al desarrollo integral del asociado mediante la prestación de servicios financieros y de bienestar.

5.2 Fase 2: Identificación del Riesgo empresa Femluker

Considerando los registros (logs) obtenidos de las herramientas tecnológicas se toma de referencia la **Tabla 4-3** correspondientes a la empresa Femluker y se establece la **Tabla 5-2**.

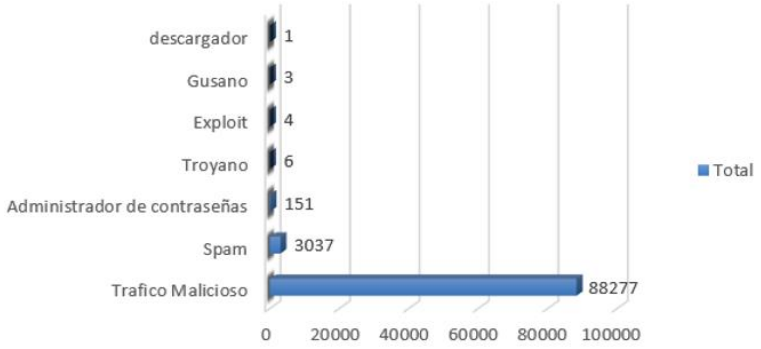
Tabla 5-2. Amenazas detectadas empresa FemLuker

#	Categoría de amenaza	Cuantas tipologías – ver (**Anexo D**)	Número de ocurrencias
1	Inadecuada gestión de contraseñas	1 tipo	27
3	Descargador	1 tipo	1
5	Exploit	1 tipo	4
6	Gusano	1 tipo	3
11	Spam	805 tipo según su procedencia	3037
12	Trafico Malicioso	69 tipos	88277
13	Troyano	1 tipo	6

De esta forma, se construye la matriz que se encuentra en el (**Anexo E**) con base en la información de la **Ilustración 5-1** y el cruce con los activos de la **Tabla 5-1** que son

considerados de importancia para la ejecución de sus operaciones. Por tanto, se obtienen 44 escenarios de riesgos a las que se les determinará la gravedad del riesgo.

Ilustración 5-1. Amenazas detectadas empresa FemLuker



5.3 Fase 3: Determinación de la gravedad del Riesgo de la empresa FemLuker

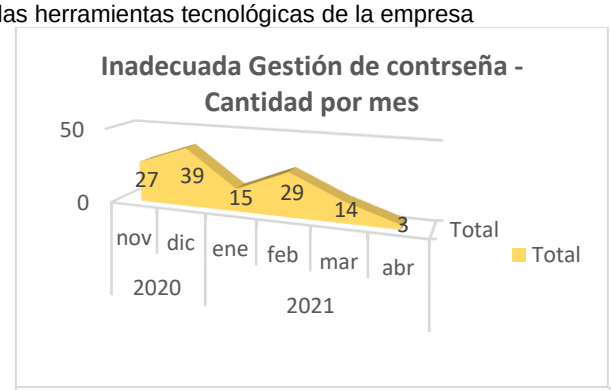
5.3.1 Gravedad del Riesgo = Probabilidad x Impacto

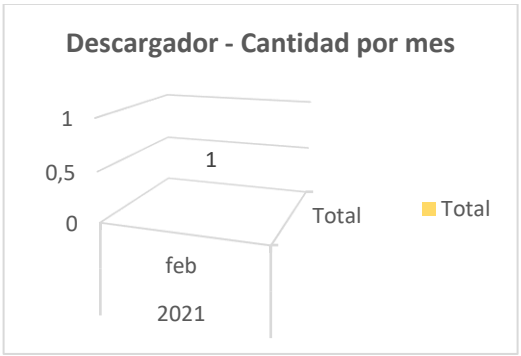
Siguiendo el plan establecido en la propuesta, se procede a obtener la Gravedad del Riesgo de cada escenario construido en el paso anterior. De tal forma, se procede a dar la puntuación de los conceptos de los Factores de Agente de Amenaza que son el Nivel de habilidad, Motivación, Oportunidad y Tamaño como se estableció en la **Ilustración 4-4**. Este último, se toma en cuenta los logs recolectados de las herramientas tecnológicas, por consiguiente, se debe crear antes de la evaluación la **Tabla 5-3**. Esta tabla, también es un insumo para los factores de vulnerabilidad establecidos en la **Ilustración 4-5** para calificar el criterio de facilidad de descubrimiento y detección de intrusiones puesto que contiene la cantidad de amenazas detectadas para la empresa en estudio en los últimos 6 meses de la toma registros (Logs). También se puede establecer una decisión en el criterio de explotación, ya que deja a muy fácil juicio la calificación según las amenazas y la cantidad de estas para que un atacante pueda aprovechar esta vulnerabilidad en función de los eventos registrados.

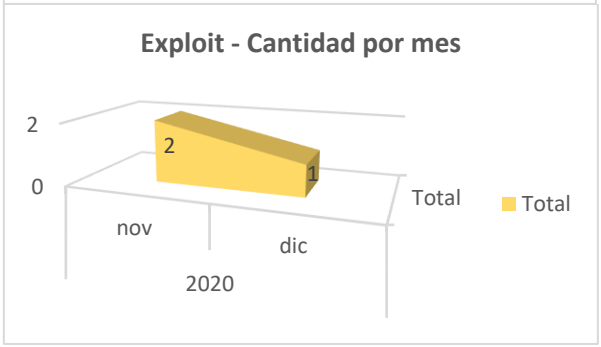
Tabla 5-3. Datos para calificar factores de agente amenaza y vulnerabilidad

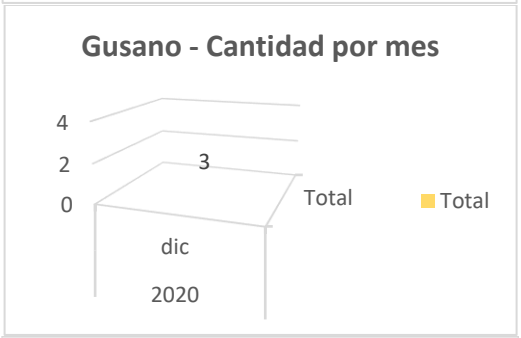
Cantidad promedio de las amenazas de los últimos seis meses (noviembre 2020 – abril 2021) en el que se recolectaron los registros (Logs) de las herramientas tecnológicas de la empresa

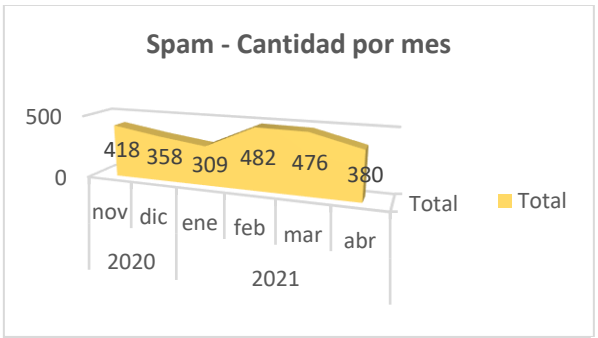
#	Amenaza	Promedio
1	Inadecuada gestión de contraseña	21,2
2	Descargador	0,2
3	Exploit	0,5
4	Gusano	0,5
5	Spam	403,8
6	Trafico Malicioso	10263,0
7	Troyano	0,5

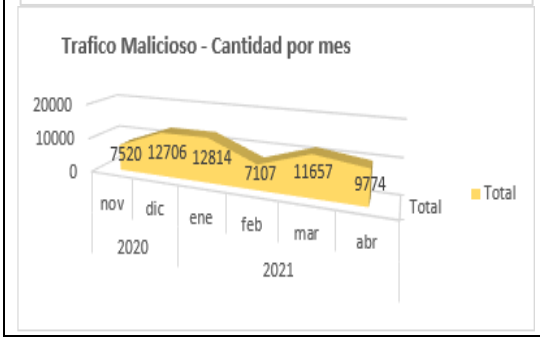


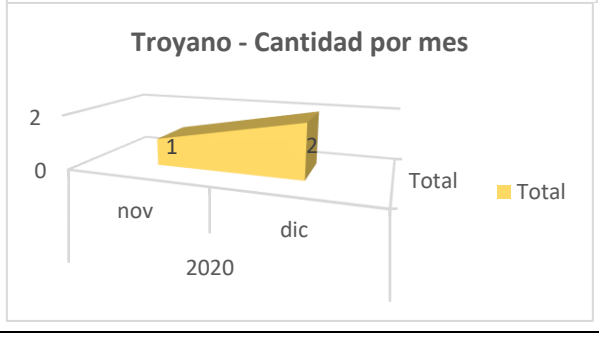








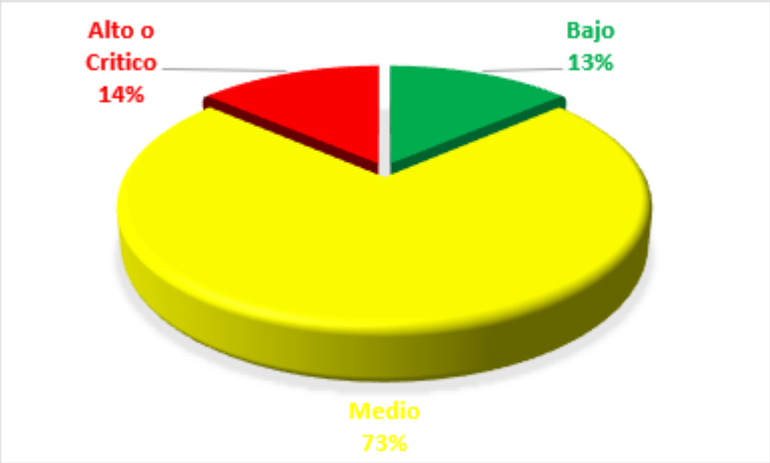




La **Tabla 5-3** nos muestra como los eventos relacionados con el Spam y trafico malicioso juegan un papel alto en ocurrencias, que por sus criterios de definición pueden dar paso a otras amenazas y que influyen en la calificación de la severidad de la gravedad como se visualiza en el (**Anexo F**).

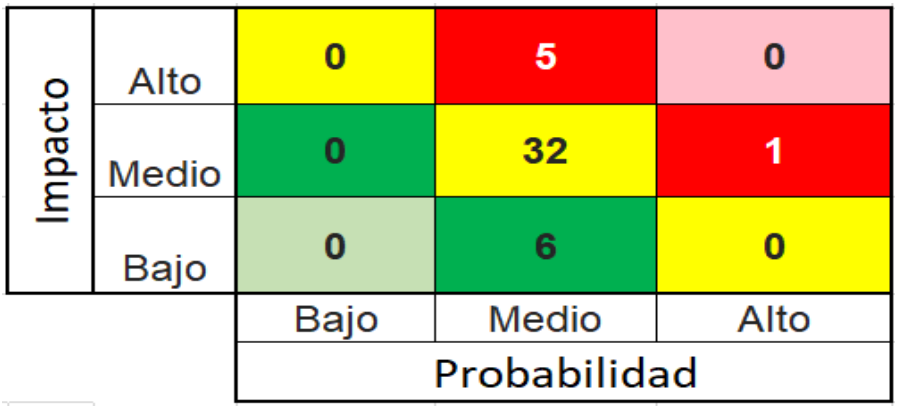
De esta forma, como se visualiza en **Ilustración 5-2.** Resultado Gravedad Riesgo FemLuker, se obtiene que, de los 44 escenarios de riesgos conformados sobre las amenazas detectadas, el 14 por ciento corresponde a una severidad alta o crítica y en un amplio porcentaje del 73% en la escala media de severidad.

Ilustración 5-2. Resultado Gravedad Riesgo FemLuker



El mapa de calor relacionado en la **Ilustración 5-3.** Mapa de calor gravedad del riesgomuestra la distribución de la severidad de los 44 escenarios de riesgos identificados para la empresa FemLuker.

Ilustración 5-3. Mapa de calor gravedad del riesgo



5.3.2 Controles para escenario riesgo con severidad alta para empresa FemLuker

El Macroproceso de la empresa FemLuker como propósito de funcionamiento es la contribución al desarrollo integral del asociado mediante la prestación de servicios financieros y de bienestar. Considerando ello y la severidad alta detectada en los escenarios de riesgos conformados se establecen controles como los visualizados en la **Tabla 5-4** y que se complementan en el (**Anexo G**). Algunos de estos están definidos en la propuesta y otros adicionales al contexto como soporte de la operación de la empresa.

Tabla 5-4. Controles propuestos para la mitigación del Riesgo encontrado

#	Escenario de riesgo con severidad alta	Descripción del Control existentes
1	Falla en funcionamiento del sistema operativo en servidores con sistema operativo (Windows Server – Windows Storage Server) o sistema operativo en equipos computo usuarios finales (Windows 10 profesional – -MacOS Catalina) que limite la ejecución de servicios por causa de una inadecuada gestión de contraseña	Para sistema operativo en servidor: Una falla en el **Sistema Operativo** donde se encuentra la Base de Datos o ERP OPA implica estimar e implementar los siguientes controles: **1.** Cambio trimestral de **contraseñas** del acceso al servidor y aplicativo OPA. **2.** Considerando el servidor virtual donde está la BD se debe **aplicar copia de la maquina virtual** periódicamente (todas las noches) para restablecimiento ante errores que impadan arrancar el sistema operativo del servidor y en el caso del **servidor físico** implementar **copia** semanal de la maquina física de forma virtual para dado el caso levantar servicios dentro de un servidor virtual. Para sistema operativo equipos cómputos usuario final: Aplica punto1. adicional, **crear una imagen del sistema en equipo computo** para levantar el recursos computo en un menor tiempo posible
2	Daños fortuitos de la información en base de datos SQL. Alteración de datos, perdida total o parcial de información por una inadecuada gestión de contraseñas	**1.** Aplicar política de **cambio periódico de contraseña** en usuarios que usan el aplicativo. **2**. **Copia seguridad** periódica (cada noche)
3	Daños fortuitos de la información en base de datos SQL. Alteración de datos, perdida total o parcial de información por cuenta de un gusano	**1. Copia seguridad** periódica (cada noche)
#	Escenario de riesgo con severidad alta	Descripción del Control existentes
4	Alteración de datos, perdida total o parcial de información por acceso indebido al sistema de información (OPA) por una inadecuada gestión de contraseña	**1.** Aplicar política de **cambio periódico de contraseña** en usuarios que usan el aplicativo.
5	Alteración de datos, perdida total o parcial de información por acceso indebido al sistema de información (OPA) por cuenta de un gusano	**1. Copia seguridad** periódica (cada noche)
6	Afectación de la red corporativa en el marco de seguridad perimetral por cuenta de un trafico malicioso	**1.** Generación de Reporte bimestral para evaluar trafico y aplicar restricciones sobre procedencias dudas o trafico no reconocido

5.3.3 Riesgo Residual

El (**Anexo G**) contiene el resultado de aplicar nuevamente la evaluación de los factores de probabilidad e impacto. Se cumple con el propósito de disminuir los riesgos con los controles mencionados en la **Tabla 5-4**. Los seis escenarios de riesgos que estaban con la calificación de severidad alta cambian a 4 en severidad media, seguido de 2 en bajo como se detalla en **Ilustración 5-4.** Severidad del riesgo por controles existentes

Ilustración 5-4. Severidad del riesgo por controles existentes

5.4 Determinar que arreglar

FemLuker es una empresa que depende del área de tecnología de la información que debe invertir en la seguridad de la información de sus procesos críticos para garantizar la operación de la compañía, considerando el aporte que el entorno multi empresarial genera. Este tipo de inversiones pueden verse representadas de alguna forma como alianza estratégica con terceros, persona de planta o porcentaje de apoyo en gastos para mejorar y sostener los controles mencionados en **Tabla 5-4**. Por tanto, el (Anexo H) contiene un plan de tratamiento de riesgos propuesto y que debe ser analizado por las directivas que gobiernan la empresa para establecer la viabilidad en una inversión anual de 55.328.650 pesos aproximadamente.

Conclusiones y recomendaciones

5.5 Conclusiones

Los marcos metodológicos de gestión del riesgo mencionados en el documento poseen estrategias que apuntan al ajuste de medidas de seguridad de la información y como a partir de ellos adaptarlos a las operaciones de una organización. OWASP un marco flexible que alineado con las vulnerabilidades e incidencias de las herramientas tecnológicas contribuye a la estandarización de un plan de seguridad resaltando la importancia de invertir en tecnología.

Las herramientas tecnológicas que pueden tener instaladas las compañías para sostener la operatividad principal de su proceso macro, fueron un suministro muy importante, ya que se obtuvieron valores cuantitativos sobre hechos reales. Facilitando así, una calificación más objetiva sobre los escenarios de riesgos. Por tanto, La contribución de los registros (Logs) apoyaron el marco metodológico OWASP en el diseño de la propuesta metodológica.

La propuesta aplicada a la empresa FemLuker evidencia la estructura lograda del marco metodológico OWASP mediante la inclusión de datos reales. Puesto que, permitió calificar los criterios de los factores de agentes de amenaza y de vulnerabilidad de una forma más asertiva, evadiendo en un buen porcentaje la subjetividad para aplicar la determinación de lo que se debe ajustar como parte del plan de mitigación e inversión que la empresa debe considerar.

El marco de Gestión de Riesgo de Tecnologías de la Información y Comunicación del entorno multi empresarial basado en toma de registros (Logs) si apoya a la toma de

decisiones corporativas hacia la protección de la seguridad de la información que también sirve como un suministro ante las auditorias o certificaciones que puedan tener las empresas del entorno.

5.6 Recomendaciones

Las metodologías, marcos y normas de gestión de riesgos en seguridad de la información deberían contemplar un suministro tangible de información como lo es la toma de registros (Logs) de las herramientas tecnológicas existentes en una organización, para modelar a partir de allí referentes en el establecimiento de rutas de trabajo estructurado de riesgo en función de los eventos.

Un referente para evaluar a futuras investigaciones es la visualización de un análisis de cómo afecta positiva o negativamente la inclusión de análisis de registros (logs) en las metodologías, marcos y normas de gestión de riesgos en seguridad de la información que se encuentren vigentes, al igual lo que implica esta actividad para funcionarios del área de Tecnología de la Información y en recursos tecnológicos.

Adicional, se sugiere el desarrollo o adquisición de una herramienta o aplicación que puede aportar en la evaluación de las matrices recolectadas de gestión de riesgos considerando las evidencias a partir de (logs), de tal forma que se adquiera habilidades competentes y objetivas para establecer deliberaciones en función de las estrategias que se debiesen aplicar para la mitigación del riesgo.

A. Anexo: Tipología de amenazas

En la carpeta anexos se encuentra el archivo digital en Excel con el nombre de 1. Entregable Logs Amenazas.xlsx

B. Anexo: Escenarios de riesgos

			Amenazas													
Capa	**#**	**Activos**	**Inadecuada gestión de contraseña**	**Clicker de troyano**	**Descargador**	**Dropper**	**Exploit**	**Gusano**	**Ofuscator**	**Puerta trasera**	**Rasomware**	**Software de seguridad no deseado**	**Spam**	**Trafico Malicioso**	**Troyano**	**Virus de Macro**
Centro de redes y cableado	1	Switch o dispositivos de red								Falla o daño en dispositivo switch o dispositivo de red por puertas traseras abiertas				Falla o daño en dispositivo switch o dispositivo de red por tráfico malicioso		
	2	Enlace Comunicaciones								Falla en los enlaces de comunicaciones para voz y datos por puertas traseras abiertas				Falla en los enlaces de comunicaciones para voz y datos por tráfico malicioso		

Servidores (Físicos, Virtuales y en la nube)	3	Servidores físicos y virtuales	Falla o perdida de hardware de los servidores físicos y virtuales por inadecuada gestión de contraseña				Falla o perdida de hardware de los servidores físicos y virtuales por cuenta de Exploit		Falla o perdida de hardware de los servidores físicos y virtuales por cuenta de ofuscador	Falla o perdida de hardware de los servidores físicos y virtuales por cuenta de puertas traseras abiertas		Falla o perdida de hardware de los servidores físicos y virtuales por cuenta de software de seguridad no deseado		Falla o perdida de hardware de los servidores físicos y virtuales por cuenta de tráfico malicioso	Falla o perdida de hardware de los servidores físicos y virtuales por cuenta de troyanos	
	4	NAS	Falla o perdida de hardware del equipo NAS por cuenta de una inadecuada gestión de contraseña							Falla o perdida de hardware del equipo NAS por cuenta de puerta trasera				Falla o perdida de hardware del equipo NAS por cuenta de puerta trasera		

Pc's escritorio e impresoras	5	Equipos computo usuario final	Pérdida total o parcial de información en equipos computo de usuario final por cuenta de una inadecuada gestión de contraseña	Pérdida total o parcial de información en equipos computo de usuario final por cuenta de un Clicker de troyano	Pérdida total o parcial de información en equipos computo de usuario final por cuenta de una amenaza descargadora	Pérdida total o parcial de información en equipos computo de usuario final - Fallas Hardware del equipo computo del usuario final por cuenta de un Dropper	Pérdida total o parcial de información en equipos computo de usuario final por cuenta de un Exploit	Pérdida total o parcial de información en equipos computo de usuario final por cuenta de un gusano	Pérdida total o parcial de información en equipos computo de usuario final por cuenta de un Ofuscator	Pérdida total o parcial de información en equipos computo de usuario final por cuenta de una puerta trasera abierta	Pérdida total o parcial de información en equipos computo de usuario final de un Rasomware	Pérdida total o parcial de información en equipos computo de usuario final de un software de seguridad no deseado	Pérdida total o parcial de información en equipos computo de usuario final por cuenta de Spam malicioso		Pérdida total o parcial de información en equipos computo de usuario final por cuenta de troyano	Pérdida total o parcial de información en equipos computo de usuario final por cuenta de virus macro

Sistemas operativos	6	Windows Server + Windows Storage Server + Windows 10 Professional	Falla en funcionamiento del sistema operativo en servidores con sistema operativo (Windows Server - Windows Storage Server) o sistema operativo en equipos computo usuarios finales (Windows 10 profesional - - MacOS Catalina) que limite la ejecución de servicios por	Falla en funcionamiento del sistema operativo en servidores con sistema operativo (Windows Server - Windows Storage Server) o sistema operativo en equipos computo usuarios finales (Windows 10 profesional - - MacOS Catalina) que limite la ejecuci	Falla en funcionamiento del sistema operativo en servidores con sistema operativo (Windows Server - Windows Storage Server) o sistema operativo en equipos computo usuarios finales (Windows 10 profesional - - MacOS Catalina) que limite la ejecución de servicios por	Falla en funcionamiento del sistema operativo en servidores con sistema operativo (Windows Server - Windows Storage Server) o sistema operativo en equipos computo usuario finales (Windows 10 profesional - - MacOS Catalina) que limite la ejecuci	Falla en funcionamiento del sistema operativo en servidores con sistema operativo (Windows Server - Windows Storage Server) o sistema operativo en equipos computo usuarios finales (Windows 10 profesional - - MacOS Catalina) que limite la ejecución de servicios por	Falla en funcionamiento del sistema operativo en servidores con sistema operativo (Windows Server - Windows Storage Server) o sistema operativo en equipos computo usuarios finales (Windows 10 profesional - - MacOS Catalina) que limite la ejecución de servicios por	Falla en funcionamiento del sistema operativo en servidores con sistema operativo (Windows Server - Windows Storage Server) o sistema operativo en equipos computo usuario finales (Windows 10 profesional - - MacOS Catalina) que limite la ejecuci	Falla en funcionamiento del sistema operativo en servidores con sistema operativo (Windows Server - Windows Storage Server) o sistema operativo en equipos computo usuarios finales (Windows 10 profesional - - MacOS Catalina) que limite la ejecución de	Falla en funcionamiento del sistema operativo en servidores con sistema operativo (Windows Server - Windows Storage Server) o sistema operativo en equipos computo usuarios finales (Windows 10 profesional - - MacOS Catalina) que limite la ejecución de servicios por	Falla en funcionamiento del sistema operativo en servidores con sistema operativo (Windows Server - Windows Storage Server) o sistema operativo en equipos computo usuario finales (Windows 10 profesional - - MacOS Catalina) que limite la ejecuci			Falla en funcionamiento del sistema operativo en servidores con sistema operativo (Windows Server - Windows Storage Server) o sistema operativo en equipos computo usuarios finales (Windows 10 profesional - - MacOS Catalina) que limite la ejecución de servicios por	

			causa de una inadecuada gestión de contraseña	ón de servicios por causa de un Clicker de troyano	cuenta de una amenaza descargadora	ón de servicios por cuenta de un Dropper	cuenta de un Exploit	cuenta de un gusano	ón de servicios por cuenta de un Ofuscator	servicios por cuenta de una puerta trasera abierta	cuenta de un Rasomware	ón de servicios por cuenta de un software de seguridad no deseado			cuenta de un troyano	
Motores de Bases de datos	7	Oracle + SQL + Hana	Daños fortuitos de la información en base de datos como Oracle, SQL y Hana. Alteración de datos, pérdida		Daños fortuitos de la información en base de datos como Oracle, SQL y Hana. Alteración de datos, pérdida		Daños fortuitos de la información en base de datos como Oracle, SQL y Hana. Alteración de datos, pérdida	Daños fortuitos de la información en base de datos como Oracle, SQL y Hana. Alteración de datos, pérdida	Daños fortuitos de la información en base de datos como Oracle, SQL y Hana. Alteración de	Daños fortuitos de la información en base de datos como Oracle, SQL y Hana. Alteración de datos, pérdida	Daños fortuitos de la información en base de datos como Oracle, SQL y Hana. Alteración de datos, pérdida				Daños fortuitos de la información en base de datos como Oracle, SQL y Hana. Alteración de datos, pérdida	Daños fortuitos de la información en base de datos como Oracle, SQL y Hana. Alteración de datos, pérdida

			total o parcial de información por una inadecuada gestión de contraseña		total o parcial de información por una amenaza descargadora		total o parcial de información por cuenta de un Exploit	total o parcial de información por cuenta de un gusano	datos, pérdida total o parcial de información por cuenta de un Ofuscator	total o parcial de información por cuenta de una puerta trasera abierta	total o parcial de información por cuenta de un Rasomware				total o parcial de información por cuenta de un troyano	total o parcial de información por cuenta de un virus macro
Sistemas de información Transaccionales	8	SAP + Queryx 7 + OPA + Daruma + Agrowin	Alteración de datos, pérdida total o parcial de información por acceso indebido a los sistemas de información (SAP + Queryx 7 + OPA + Daruma + Agrowin) por una inadecuada		Alteración de datos, pérdida total o parcial de información por acceso indebido a los sistemas de información (SAP + Queryx 7 + OPA + Daruma + Agrowin) por cuenta de una amenaz		Alteración de datos, pérdida total o parcial de información por acceso indebido a los sistemas de información (SAP + Queryx 7 + OPA + Daruma + Agrowin) por cuenta de un Exploit	Alteración de datos, pérdida total o parcial de información por acceso indebido a los sistemas de información (SAP + Queryx 7 + OPA + Daruma + Agrowin) por cuenta de un gusano	Alteración de datos, pérdida total o parcial de información por acceso indebido a los sistemas de información (SAP + Queryx 7 + OPA + Daruma + Agrowin) por cuenta de un	Alteración de datos, pérdida total o parcial de información por acceso indebido a los sistemas de información (SAP + Queryx 7 + OPA + Daruma + Agrowin) por cuenta de una	Alteración de datos, pérdida total o parcial de información por acceso indebido a los sistemas de información (SAP + Queryx 7 + OPA + Daruma + Agrowin) por cuenta de un				Alteración de datos, pérdida total o parcial de información por acceso indebido a los sistemas de información (SAP + Queryx 7 + OPA + Daruma + Agrowin) por cuenta de un troyano	Alteración de datos, pérdida total o parcial de información por acceso indebido a los sistemas de información (SAP + Queryx 7 + OPA + Daruma + Agrowin) por cuenta de un

			gestión de contraseña		a descargadora				Ofuscator	puerta trasera abierta	Rasomware						virus macro
Servicios de TI	9	Comunicaciones (Internet – Canal de datos – Telefonía)								Falla o deficiencia en funcionamiento de las Comunicaciones (Internet - Canal de datos - Telefonía) por cuenta de una puerta trasera abierta				Falla o deficiencia en funcionamiento de las Comunicaciones (Internet - Canal de datos - Telefonía) por cuenta de un tráfico malicioso		

	10	Colaborativos (Correo Electrónico – mensajería instantánea)	Perdida de información o suplantación de identidad para fines ilícitos de las herramientas colaborativas (Correo Electrónico - mensajería instantánea) por cuenta de una inadecuada gestión de contraseña	Perdida de información o suplantación de identidad para fines ilícitos de las herramientas colaborativas (Correo Electrónico - mensajería instantánea) por cuenta de un Clicker de troyano	Perdida de información o suplantación de identidad para fines ilícitos de las herramientas colaborativas (Correo Electrónico - mensajería instantánea) por cuenta de una amenaza descargadora	Perdida de información o suplantación de identidad para fines ilícitos de las herramientas colaborativas (Correo Electrónico - mensajería instantánea) por cuenta de un Droppe r	Perdida de información o suplantación de identidad para fines ilícitos de las herramientas colaborativas (Correo Electrónico - mensajería instantánea) por cuenta de un Exploit	Perdida de información o suplantación de identidad para fines ilícitos de las herramientas colaborativas (Correo Electrónico - mensajería instantánea) por cuenta de un gusano	Perdida de información o suplantación de identidad para fines ilícitos de las herramientas colaborativas (Correo Electrónico - mensajería instantánea) por cuenta de un Ofuscator	Perdida de información o suplantación de identidad para fines ilícitos de las herramientas colaborativas (Correo Electrónico - mensajería instantánea) por una puerta trasera abierta	Perdida de información o suplantación de identidad para fines ilícitos de las herramientas colaborativas (Correo Electrónico - mensajería instantánea) por cuenta de un Rasomware	Perdida de información o suplantación de identidad para fines ilícitos de las herramientas colaborativas (Correo Electrónico - mensajería instantánea) por cuenta de un softwar e de seguridad no deseado	Perdida de información o suplantación de identidad para fines ilícitos de las herramientas colaborativas (Correo Electrónico - mensajería instantánea) por spam malicioso		Perdida de información o suplantación de identidad para fines ilícitos de las herramientas colaborativas (Correo Electrónico - mensajería instantánea) por cuenta de un troyano	Perdida de información o suplantación de identidad para fines ilícitos de las herramientas colaborativas (Correo Electrónico - mensajería instantánea) por cuenta de un virus macro
	11	Seguridad Perimetral	Afectación de la red corporativa en el marco				Afectación de la red corporativa en el marco	Afectación de la red corporativa en el marco		Afectación de la red corporativa en el marco				Afectación de la red corporativa en el marco		

			de seguridad perimetral por una inadecuada gestión de la contraseña				de seguridad perimetral por cuenta de un Exploit	de seguridad perimetral por cuenta de un gusano		de seguridad perimetral de una puerta trasera abierta				de seguridad perimetral por cuenta de un tráfico malicioso		
	12	Almacenamiento (NAS)	Pérdida total o parcial de información en equipos de almacenamiento NAS por inadecuada gestión de contraseñas				Pérdida total o parcial de información en equipos de almacenamiento NAS por cuenta de un Exploit	Pérdida total o parcial de información en equipos de almacenamiento NAS por cuenta de un gusano			Pérdida total o parcial de información en equipos de almacenamiento NAS por cuenta de un Rasomware				Pérdida total o parcial de información en equipos de almacenamiento NAS por cuenta de un troyano	Pérdida total o parcial de información en equipos de almacenamiento NAS por cuenta de un virus macro

	13	Suite office 365	Perdida de información en la nube en el uso de SharePoint o Onedrive de la suite office 365 por inadecuada gestión de la contraseña	Perdida de información en la nube en el uso de SharePoint o Onedrive de la suite office 365 por cuenta de un Clicker troyano	Perdida de información en la nube en el uso de SharePoint o Onedrive de la suite office 365 por una amenaza descargadora	Perdida de información en la nube en el uso de SharePoint o Onedrive de la suite office 365 por cuenta de un Droppe r	Perdida de información en la nube en el uso de SharePoint o Onedrive de la suite office 365 por cuenta de un Exploit	Perdida de información en la nube en el uso de SharePoint o Onedrive de la suite office 365 por cuenta de un gusano	Perdida de información en la nube en el uso de SharePoint o Onedrive de la suite office 365 por cuenta de un Ofuscator	Perdida de información en la nube en el uso de SharePoint o Onedrive de la suite office 365 por cuenta de una puerta trasera	Perdida de información en la nube en el uso de SharePoint o Onedrive de la suite office 365 por cuenta de un Rasomware	Perdida de información en la nube en el uso de SharePoint o Onedrive de la suite office 365 por cuenta de un software de seguridad no deseado	Perdida de información en la nube en el uso de Share Point o Onedrive de la suite office 365 por cuenta de un Spam malicioso		Perdida de información en la nube en el uso de SharePoint o OneDrive de la suite office 365 por cuenta de un troyano	Perdida de información en la nube en el uso de SharePoint o Onedrive de la suite office 365 por cuenta de un virus de macro

C. Anexo: Matriz de riesgos

En la carpeta anexos se encuentra el archivo digital en Excel con el nombre de 2. Matriz de riesgos.xlsx que contiene la depuración de los escenarios de riesgos en la hoja Def. Esc. Riesgo

D. Anexo: Tipologías de amenazas detectadas en empresa FemLuker

En la carpeta anexos se encuentra el archivo digital en Excel con el nombre de 1. Entregable logs Amenazas que contiene la clasificación de estás para la empresa FemLuker en la hoja FemLuker.

E. Anexo: Tipologías de amenazas detectadas en empresa FemLuker

En la carpeta anexos se encuentra el archivo digital en Excel con el nombre de 2. Matriz de riesgos en la hoja Def. Esc. Riesgo – Femluker.

F. Anexo: Severidad del riesgo detectado para la empresa FemLuker

En la carpeta anexos se encuentra el archivo digital en Excel con el nombre de 2. Matriz de riesgos en la hoja Severidad Riesgo - FemLuker.

G. Anexo: Aplicación de controles existentes para la empresa FemLuker

En la carpeta anexos se encuentra el archivo digital en Excel con el nombre de 2. Matriz de riesgos en la hoja Controles + Ries. Residual.

H. Anexo: Aplicación de controles existentes para la empresa FemLuker

#	Escenario de Riesgo	Severidad del Riesgo al implementar el control	Estrategia de Tratamiento	Responsable	Fecha cierre	Seguimiento		Costo Aprox. Inversión primer año
						Estado	Observaciones	
1	Falla en funcionamiento del sistema operativo en servidores con sistema operativo (Windows Server - Windows Storage Server) o sistema operativo en equipos computo usuarios finales (Windows 10 profesional - - MacOS Catalina) que limite la ejecución de servicios por causa de una inadecuada gestión de contraseña	MEDIO	**Para temas sistemas operativos en servidores:** Bajo una política de seguridad corporativa solo el Administrador del servidor está autorizado para aplicar configuraciones que en conjunto con el proveedor de la aplicación deban realizar y documentar // **Para temas sistemas operativos en equipos computo usuario final:** identificar usuarios críticos que deban implementar doble factor de autenticación como medida de seguridad que trae el directorio activo en sincronización con la suite de office 365 // Aplicar copia de seguridad a usuarios críticos para restablecimiento de la información al dañarse sistema operativo (Licencia GreenBackup)	Gerente Femluker + jefe del área de Tecnología de la Información	Permanente	Propuesta	Sujeto a decisiones corporativas costo beneficio para ejecución del tratamiento	$ 1.328.650,00

2	Daños fortuitos de la información en base de datos SQL. Alteración de datos, pérdida total o parcial de información por una inadecuada gestión de contraseñas	MEDIO	Establecer un área o persona responsable de manejar la seguridad informática de la Compañía con monitoreo y controles permanentes.	Gerente Femluker + jefe del área de Tecnología de la Información	Permanente	Propuesta	Sujeto a decisiones corporativas costo beneficio para ejecución del tratamiento	$ 36.000.000,00
3	Daños fortuitos de la información en base de datos SQL. Alteración de datos, pérdida total o parcial de información por cuenta de un gusano	BAJO	No aplica controles adicionales	Gerente Femluker + jefe del área de Tecnología de la Información	Permanente	Propuesta	Sujeto a decisiones corporativas costo beneficio para ejecución del tratamiento	$ -
4	Alteración de datos, pérdida total o parcial de información por acceso indebido al sistema de información (OPA) por una inadecuada gestión de contraseña	MEDIO	No aplica controles adicionales	Gerente Femluker + jefe del área de Tecnología de la Información	Permanente	Propuesta	Sujeto a decisiones corporativas costo beneficio para ejecución del tratamiento	$ -
5	Alteración de datos, pérdida total o parcial de información por acceso indebido al sistema de información (OPA)	BAJO	Servidor alterno con imagen virtual para reestablecer sistema con copia	Gerente Femluker + jefe del área de Tecnología de la Información	Permanente	Propuesta	Sujeto a decisiones corporativas costo beneficio para ejecución del tratamiento	$ 18.000.000,00

	por cuenta de un gusano							
6	Afectación de la red corporativa en el marco de seguridad perimetral por cuenta de un tráfico malicioso	MEDIO	Establecer un área o persona responsable de manejar la seguridad informática de la Compañía con monitoreo y controles permanentes. Ya establecido en escenario 2	Gerente Femluker + jefe del área de Tecnología de la Información	Permanente	Propuesta	Sujeto a decisiones corporativas costo beneficio para ejecución del tratamiento	$ -
							Total	**$ 55.328.650,00**

Bibliografía

Agrawal, V. (2017). A Comparative Study on Information Security Risk Analysis Methods. *Journal of Computers*, *12*(1), 57–67. https://doi.org/10.17706/jcp.12.1.57-67

Almanza J., A. R. (2019). XIX Encuesta Nacional de Seguridad Informática. *Revista Sistemas*, *151*, 12–41. https://doi.org/10.29236/sistemas.n151a3

Amutio Gómez, M. A. (2012). *Ministerio de Hacienda y Administraciones Publicas*. 127. http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

B. S., K., SRIDHAR, V., & K. R., S. (2019). a Case Study: Risk Rating Methodology for E-Governance Application Security Risks. *I-Manager's Journal on Software Engineering*, *13*(3), 39. https://doi.org/10.26634/jse.13.3.15546

Benavides, E., Fuertes, W., & Sanchez, S. (2020). Caracterización de los ataques de phishing y técnicas para mitigarlos. Ataques: una revisión sistemática de la literatura. *Ciencia y Tecnología*, *13*(1), 97–104. https://doi.org/10.18779/cyt.v13i1.357

Bornman, W. G., & Labuschagne, L. (2004). A comparative framework for evaluating information security risk management methods. *Information Security South Africa Conference*. http://icsa.cs.up.ac.za/issa/2004/Proceedings/Full/015.pdf

Burkert, R., van Hagen, J., Wehrmann, M., & Jansen, M. (2022). Protection Against Online Fraud Using Blockchain. In *Lecture Notes in Networks and Systems: Vol. 320 LNNS* (pp. 34–43). https://doi.org/10.1007/978-3-030-86162-9_4

Centro de seguridad y cumplimiento - Service Descriptions | Microsoft Docs. (n.d.). Retrieved July 14, 2021, from https://docs.microsoft.com/es-es/office365/servicedescriptions/office-365-platform-service-description/office-365-securitycompliance-center

CONPES. (2016). Política Nacional de Seguridad Digital. *CONPES 3854 - Política Nacional de Seguridad Digital*, 91. https://colaboracion.dnp.gov.co/CDT/Conpes/Economicos/3854.pdf

Edgard Pujaico Paredes, M. (2018). *"MODELO DE GESTIÓN DE SERVICIOS DE CONTROL PARA EL ÓRGANO DE CONTROL INSTITUCIONAL DE LA SUPERINTENDENCIA DEL MERCADO DE VALORES."*

ENISA. (2006). Inventory of risk assessment and risk management methods. *ENISA Ad Hoc Working Group on Risk Assessment and Risk Management*, 1–56.

http://www.enisa.europa.eu/act/rm/files/deliverables/inventory-of-risk-assessment-and-risk-management-methods/at_download/fullReport

Fabisiak, L., Hyla, T., & Klasa, T. (2012). Comparative Analysis of Information Security Assessment and Management Methods. *Studia i Materialy Polskiego Stowarzyszenia Zarzadzania Wiedza / Studies & Proceedings Polish Association for Knowledge Management*, *60*, 55–70.

FERMA. (2003). *Estándares de Gerencia de Riesgo (1)*.

Flores Urgilés, C., Zhinin Aguayza, B., Segovia Cantos, A., Mayancela Zhinin, M., & Marlene García, J. (2018). Evaluación de seguridad de la información en las páginas web pertenecientes a los municipios de la provincia del Cañar. *Killkana Técnica*, *2*(1), 13. https://doi.org/10.26871/killkana_tecnica.v2i1.286

Fortinet. (n.d.-a). Is Your Data Center Ready for Machine Learning Hardware? *White Paper*. https://www.datacenterknowledge.com/machine-learning/your-data-center-ready-machine-learning-hardware

Fortinet. (n.d.-b). *Next-Generation Firewall (NGFW)* | *Fortinet*. Retrieved July 15, 2021, from https://www.fortinet.com/lat/products/next-generation-firewall

Fortinet. (2021a). *Technical Tip : FortiGate - UDP Flooding Attack is blocked but amount of traffic does not decrease*. 9–10.

Fortinet. (2021b). *Threat Encyclopedia* | *FortiGuard*. https://www.fortiguard.com/encyclopedia/ips/100663398

Fortinet. (2021c). *What is ICMP (Internet Control Message Protocol)?* | *Fortinet*. https://www.fortinet.com/lat/resources/cyberglossary/internet-control-message-protocol-icmp

Fortinet. (2021d). *What Is Unified Threat Management (UTM)?* | *Fortinet*. https://www.fortinet.com/resources/cyberglossary/unified-threat-management

Fuentes, L. F. (2008). Malware, una amenaza de Internet. *Revista Digital Universitaria*, *9*(4), 1–9.

ISO/IEC. (2009). Information technology - Security techniques - Information security management systems - Overview and vocabulary. *Iso/Iec*, *2009*, ISO/IEC 27000:2009(E). https://www.iso.org/standard/73906.html

ISO/IEC 27000. (2018). International Standard ISO / IEC Information technology — Security techniques — Information security management systems — Overview and. *ACM Workshop on Formal Methods in Security Engineering.Washington, DC, USA*, *34*(19), 45–55. https://doi.org/10.1016/j.im.2003.02.002

ISO 31000. (2018). *ISO 31000:2018(es), Gestión del riesgo — Directrices*. https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es

López, M. de los Á., Albanese, D. E., & Sánchez, M. A. (2014). *Gestión de riesgos para la adopción de la computación en nube en entidades financieras de la República argentina*. Contaduria y Administracion. https://doi.org/10.1016/s0186-1042(14)71266-5

Marsh. (2019). 2019 Global Cyber Risk Perception Survey. *Microsoft Insights*, *September*, 1–36. https://www.marsh.com/us/insights/research/marsh-microsoft-cyber-survey-report-2019.html

Microsoft. (2021a). *Anti-spam protection - Office 365 | Microsoft Docs*. https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-spam-protection?view=o365-worldwide

Microsoft. (2021b). *Cómo Identifica Microsoft malware y aplicaciones potencialmente no deseadas - Windows security | Microsoft Docs*. https://docs.microsoft.com/es-es/windows/security/threat-protection/intelligence/criteria

Microsoft. (2021c). *Cyberthreats, viruses, and malware - Microsoft Security Intelligence*. 2021. https://www.microsoft.com/en-us/wdsi/threats

Microsoft. (2021d). *Nombres de malware - Windows security | Microsoft Docs*. Microsoft. https://docs.microsoft.com/es-es/windows/security/threat-protection/intelligence/malware-naming

Mingers, J. (2006). Realising Systems Thinking : Knowledge and Action in Management Science OR and Systems Thinking for Community Development Participatory Policy Design and Governance for a Global Age. In *Order A Journal On The Theory Of Ordered Sets And Its Applications*.

MinTIC, M. de las T. y las T. (2015). Modelo de Seguridad y Privacidad de la Información. *Diario Oficial*, 1–32. http://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_Seguridad.pdf

MinTIC, M. de las T. y las T. (2016). Modelo de Seguridad y Privacidad de La Información - Guía de Mejora Continua. *Diario Oficial*, 58. https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf%0Ahttps://www.mintic.gov.co/gestionti/615/articles-5482_G17_Mejora_continua.pdf

Munir, R., Mufti, M. R., Awan, I., Hu, Y. F., & Disso, J. P. (2015). Detection, mitigation and quantitative security risk assessment of invisible attacks at enterprise network. *Proceedings - 2015 International Conference on Future Internet of Things and Cloud, FiCloud 2015 and 2015 International Conference on Open and Big Data, OBD 2015*, 256–263. https://doi.org/10.1109/FiCloud.2015.24

Olivares, B., & Eduardo, G. (n.d.). *MODELADO DE AMENAZAS, UNA TÉCNICA DE ANÁLISIS Y GESTIÓN DE RIESGO ASOCIADO A SOFTWARE Y APLICACIONES*.

Owasp. (2013). *OWASP Risk Rating Methodology*. Owasp.

https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

OWASP. (2021). *OWASP Top Ten Web Application Security Risks | OWASP*. https://owasp.org/www-project-top-ten/

OWASP Top 10-2017. (2003). https://github.com/OWASP/Top10/issues

PANDEY, S. K. (2012). A Comparative Study of Risk Assessment Methodologies for Information Systems. *Bulletin of Electrical Engineering and Informatics*, *1*(2), 111–122. https://doi.org/10.12928/eei.v1i2.231

Pinzon G., L. C., Talero M., M. B., & Bohada, J. A. (2013). Intrusion Test and Open Source. *Revista Ciencia, Innovacion y Tegnologia (RCYIT)*, *1*(Enero-Diciembre), 25–38.

Schoenfield, B. (2015). Information Security Risk. In *Securing Systems* (Issue 5). Springer International Publishing. https://doi.org/10.1201/b18465-7

Singh, U. K., & Joshi, C. (2018). Comparative Study of Information Security Risk Assessment Frameworks. *International Journal of Computer Application*, *2*(8). https://doi.org/10.26808/rs.ca.i8v2.08

Sophos. (2012). *Endpoint Protection*. https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=418004dd-c06e-41e6-b268-27dbcb5d2fe1&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments

Sophos. (2021a). *Protección PUA y seguridad adware. Detección y limpieza de amenazas PUA*. Sophos. https://www.sophos.com/es-es/threat-center/threat-analyses/adware-and-puas.aspx

Sophos. (2021b). *Sophos Endpoint: Download reputation frequently asked questions*. https://support.sophos.com/support/s/article/KB-000035337?language=en_US#What-is-Download-Reputation?

Sophos Central Admin. (2021). *Tipos de evento de malware y PUA*. https://docs.sophos.com/central/Customer/help/es-es/central/Customer/concepts/EventTypes.html

Susanto, H., Almunawar, M., & Tuan, Y. (2011). Information security management system standards: A comparative study of the big five. *International Journal of Electrical Computer Sciences IJECS-IJENS*, *11*(5), 23–29.

Syalim, A., Hori, Y., & Sakurai, K. (2009). Comparison of risk analysis methods: Mehari, magerit, NIST800-30 and microsoft's security management guide. *Proceedings - International Conference on Availability, Reliability and Security, ARES 2009*, 726–731. https://doi.org/10.1109/ARES.2009.75

Tejena-Macías, M. A. (2018). Análisis de riesgos en seguridad de la información. *Polo Del Conocimiento*, *3*(4), 230. https://doi.org/10.23857/pc.v3i4.809

Valencia-Duque, F. J., & Orozco-Alzate, M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, *22*, 73–88. https://doi.org/10.17013/risti.22.73-88

Valencia Duque, F. J. (2018). *Aseguramiento y auditoría de tecnologías de información orientados a riesgos. Un enfoque basado en estándares internacionales*. 145. https://www.uneditorial.com/aseguramiento-y-auditoria-de-tecnologias-de-informacion-orientados-a-riesgos-un-enfoque-basado-en-estandares-internacionales-informatica.html

Valencia Duque, F. J. (2021). *Sistema de gestión de seguridad de la información basado en la familia de normas iso/iec 27000*. https://www.uneditorial.com/aseguramiento-y-auditoria-de-tecnologias-de-informacion-orientados-a-riesgos-un-enfoque-basado-en-estandares-internacionales-informatica.html

Valencia, F. J., Marulanda, C. E., & Trujillo, M. L. (2016a). *Gobierno y Gestión de Riesgos de Tecnologías de Información y Aspectos diferenciadores Government and IT Risk Management and Aspects Differentiators*. *15*(2015), 65–77.

Valencia, F. J., Marulanda, C. E., & Trujillo, M. L. (2016b). *Gobierno y Gestión de Riesgos de Tecnologías de Información y aspectos diferenciadores Government and IT Risk Management y Aspects differentiators with the*. *15*(2015), 65–77.

Vorster, A., & Labuschagne, L. (2005). A framework for comparing different information security risk analysis methodologies. *Information Security*, *193*(C), 95–103. http://portal.acm.org/citation.cfm?id=1145686

Wangen, G., Hallstensen, C., & Snekkenes, E. (2018). A framework for estimating information security risk assessment method completeness: Core Unified Risk Framework, CURF. *International Journal of Information Security*, *17*(6), 681–699. https://doi.org/10.1007/s10207-017-0382-0

WEF. (2019). Informe de riesgos mundiales 2019. In *2017*. https://doi.org/10.1017/CBO9781107415324.004

Williams, J. (n.d.). *OWASP Risk Rating Methodology*. Retrieved July 22, 2021, from https://owasp.org/www-community/OWASP_Risk_Rating_Methodology

Zabawi, A. Y., Ahmad, R., & Abdul-Latip, S. F. (2015). A comparative study for risk analysis tools in information security. *ARPN Journal of Engineering and Applied Sciences*, *10*(23), 17672–17678.