# ANÁLISIS DE RIESGOS DE LOS SISTEMAS DE SEGURIDAD INFORMÁTICA DE LA EMPRESA KAPPA10 LTDA.

**ING. JUAN CARLOS BRICEÑO OSORIO**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD**

**ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA**

**ESPECIALIZACIÓN EN SEGURIDAD INFORMATICA**

**BOGOTÁ**

**2018**

# ANÁLISIS DE RIESGOS DE LOS SISTEMAS DE SEGURIDAD INFORMÁTICA DE LA EMPRESA KAPPA10 LTDA.

**ING. JUAN CARLOS BRICEÑO OSORIO**

**Trabajo de grado como requisito para optar por el título de**

**ESPECIALISTA EN SEGURIDAD INFORMATICA**

**DIRECTOR**

**PhD (c) GABRIEL MAURICIO RAMÍREZ VILLEGAS**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD**

**ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA**

**ESPECIALIZACIÓN EN SEGURIDAD INFORMATICA**

**BOGOTA**

**2018**

Nota de aceptación:

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Bogotá, 28 de noviembre de 2018

**CONTENIDO**

Pág.

## LISTA DE TABLAS

Pág.

## LISTA DE FIGURAS

Pág.

## GLOSARIO

ACTIVOS: Estos pueden ser diferentes, algunos son del tipo datos, o información, otros pueden ser parte de un proceso de uso en el negocio, así mismo, se cuenta con recursos que pueden ser activos de nivel informático.

AMENAZAS INFORMÁTICAS: Son todo aquello que puede hacer daño a la información o a los sistemas de información de una empresa o particular, tales como el malware, los hackers de sombrero negro (o Crackers), la ingeniería social, los descuidos de los mismos empleados que manejan la información (Por ejemplo contraseñas débiles o inexistentes, usuarios y contraseñas por defecto, manejo de puertos por defecto en las aplicaciones de datos sensibles, entre otras), los eventos como incendios, terremotos, o las catástrofes naturales, como los tsunamis, inundaciones, tornados, etc.

ANÁLISIS: Es un estudio profundo de un sujeto objeto o situación, teniendo como meta el conocimiento de sus fundamentos, principios y motivos, así como su creación y demás cosas enlazadas. En este particular se hará un análisis de riesgos informáticos del área operativa de la empresa Kappa10.

AUTENTICACIÓN TIPO ENTERPRISE: Este tipo de identificación en la red de unja entidad permite cumplir un objetivo fundamental de todas las empresas, y es brindar acceso controlado a sus trabajadores, permitiendo que cada persona de acuerdo con su roll y sus capacidades pueda ingresar a los recursos necesarios para realizar su labor, pero sin comprometer la seguridad informática durante el proceso.

CONTROLES: Son los métodos que se deben seguir en cada uno de los procesos que se deben llevar en el área de TI. Los controles que se implementen deben garantizar la identificación, corrección y medición del impacto de los riesgos de forma constante, permitiendo obtener información que minimice en un alto nivel el alcance del riesgo.

ENRUTAMIENTO: Es la forma en que los equipos de redes buscan un camino adecuado por medio del cual enviaran los paquetes de datos dependiendo de su

destinatario. Por ejemplo, para alcanzar la red A, el equipo de red debe conocer cuál es su siguiente salto, es decir, a quien le entregará el paquete, y después de entregarlo entonces el siguiente equipo de red debe hacer lo mismo, así hasta que llegue a su destino.

FIREWALL: Son equipos de red que actúan controlando el tráfico que se permite o deniega entre una red y otra. Pueden permitir o bloquear el acceso por puertos TCP y UDP, o basándose en direcciones IP. De acuerdo con sus políticas dará o denegará el acceso desde un dispositivo final a otro.

FORTIAUTHENTICATOR: Es un dispositivo informático del fabricante Fortinet, encargado de realizar la gestión de identidad unificada dentro de una entidad.

FORTIGATE: Es un equipo de red tipo NGFW del fabricante Fortinet, el cual cuenta con una suite muy amplia de servicios, incluyendo cosas como enrutamiento, VPN SSL y VPN IPSec, Servidor DHCP, controladora de wifi, entre otros.

FORTIWIFI: Es un equipo de red igual al FortiGate, también del mismo fabricante, pero adicionalmente cuenta con antenas de irradiación *WiFi*.

IDS: Sistema de detección de intrusiones (*Intrusion Detection System*)

IPS: Sistema de prevención de intrusiones (*Intrusion Prevention System*)

ITIL: Biblioteca de Infraestructuras de Tecnologías de Información. En esta se encuentran las buenas prácticas del ciclo de vida de un servicio de TI. Por medio de estas prácticas un administrador puede mejorar su servicio y la disponibilidad de este para alcanzar la satisfacción de sus clientes y lograr el objetivo de la compañía.

LOG: Registro de algún evento de un sistema informático, que se guarda de forma histórica.

LOGOFF: Representa la salida de un sistema informático, cuando el usuario se desconecta de este de forma intencional por algún motivo.

LOGON: Representa la entrada a un sistema informático, cuando el usuario pone sus credenciales y presiona el botón de entrar.

METODOLOGÍA DE ANÁLISIS DE RIESGOS: Representan planes para analizar y medir las amenazas y riesgos a los que se encuentra expuesta una entidad, con el propósito de establecer los procesos para analizar los sistemas o activos, sus amenazas y vulnerabilidades, y finalmente implementar una estrategia basada en controles que permitan una adecuada gestión de riesgos.

MITIGACIÓN: Se refiere a suavizar o atenuar algo negativo, para este caso serían los riesgos informáticos.

NGFW: Firewall de próxima generación. Hace el mismo trabajo que el Firewall común, pero adicionalmente incluye características como el filtrado de contenido web, filtrado de aplicaciones, funciones de antivirus perimetral, IPS e IDS, y en ocasiones un filtro antispam sencillo.

PARTNER: Socio. Se utiliza para identificar que una persona o empresa tiene un vínculo directo con otra, y por lo tanto es respaldada por esta.

POE: Potencia sobre ethernet (Power Over Ethernet). Sirve para brindar energía a un dispositivo eléctrico de red únicamente mediante el cable de red o *patch-cord*.

RIESGO INFORMÁTICO: Es todo lo que amenaza la integridad de la información, y comprende lo que son las amenazas y vulnerabilidades. Dentro de los riesgos a los que se exponen los sistemas de información, se encuentran el acceso sin autorización (controles de acceso), robo de información, riesgos de seguridad física (los equipos de trabajo), controles de acceso (personas o solo administradores), y la seguridad en las redes (interconexión de equipos en redes de información).

TICs: Tecnologías de la información y comunicación.

TRAZABILIDAD: Conjunto de elementos que permiten hacer seguimiento a las acciones de un programa o usuario, dejando ver la fecha y hora en las que se realizaron las maniobras y que cambio se hizo.

URL: Sus siglas traducen “Localizador Uniforme de Recursos” (*Uniform Resource Locator*) y sirve para encontrar los recursos en una red por medio de nombres que se ponen en la barra de direcciones de un navegador.

VPN: Red Virtual Privada. Se usan para establecer conexiones seguras entre ubicaciones remotas, existen dos tipos, sitio a sitio y cliente a sitio.

VULNERABILIDADES: Son aquellas que permiten a un atacante el acceso a los datos o la destrucción de estos. Las vulnerabilidades se pueden clasificar de varias maneras, una de ellas es dividiéndolas en grupos, como las del tipo ambiental y físico, las económicas, las educativas, y las de tipo institucional.

## RESUMEN

La empresa Kappa10 Ltda. Ubicada en Bogotá, localidad Chapinero, se encuentra en busca de la certificación ISO 27001, que como dice ICONTEC[1], solicita tener un sistema de información confiable que permita tener una trazabilidad de los activos informáticos, y explícitamente controles de acceso a los equipos de seguridad informática. Esta fue una de las necesidades detectadas desde el área operativa de la empresa, ya que uno de los riesgos más críticos en esta, es que los ingenieros utilizan el mismo usuario genérico para todos los equipos de seguridad informática que administran, lo que no cumple con el requisito mencionado en ISO 27001.

El análisis de riesgos busca detectar las amenazas actuales de la empresa Kappa10 Ltda. así como sus causas y consecuencias sobre la infraestructura tecnológica actual. El análisis se realizará de forma general sobre los procesos y organización basándose en el conjunto de normas ISO 27001 e ISO 31000, y se encaminará a proponer una solución a uno de los problemas que surge por la falta de controles de acceso y de autenticación de los ingenieros del área de operaciones.

Este análisis pretende seguir una metodología de investigación aplicada como mapa de ruta para lograr los dos principales objetivos del proyecto, entender el problema y proponer una solución acertada a este. La metodología de investigación aplicada busca seguir una secuencia lógica, comenzando por la recolección, el procesamiento y análisis de datos (Por ejemplo, los activos informáticos). Se continuaría con las fases de análisis de situación, estudio de problemática, propuesta de alternativas de solución, y finalmente la fase de evaluación, como expresan Ferreyra y Longhi[2].


[1] ICONTEC. Norma técnica ntc-iso/iec colombiana 27001 [2006]. [en línea] [citado el 16 de mayo, 2018]. Disponible en internet: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

[2] FERREYRA, Adriana y DE LONGHI, Ana Lía. Metodología de la investigación. Córdoba, Argentina: Encuentro Grupo Editor [2014]. [en línea] [citado el 16 de mayo, 2018]. Disponible en internet:

Una vez superadas las tres primeras fases, deben quedar plenamente identificados los riesgos atados a cada una de las amenazas que presentan los activos de la entidad, y sobre todo las del problema en discusión, lo que facilitará proponer la solución adecuada, para que la empresa realice la mitigación de riesgos requerida.

Posiblemente, la mitigación del riesgo de la gestión de identidad se lleve a cabo mediante un sistema de autenticación tipo Enterprise del fabricante Fortinet (FortiAuthenticator[3], físico o en máquina virtual), ya que tiene la capacidad de interactuar e integrarse con el directorio activo de Windows y con los equipos de seguridad de la marca Fortinet[4], que son los que posee, administra y soporta la empresa.

Inicialmente, se propone trabajar este proyecto en dos grandes partes, la primera incluiría las primeras cuatro fases mencionadas anteriormente, y la segunda parte contendría las dos fases restantes, y abordaría el tema de proponer la solución a implementar para mitigar al riesgo de gestión de identidad. En el proyecto se tendría como alcance únicamente la prueba piloto a manera de laboratorio controlado.

El objetivo principal de la propuesta es analizar los riesgos de seguridad informática de la empresa Kappa10, y después del análisis enfocarse principalmente en el riesgo causado a raíz de no tener una correcta gestión de identidad. Una vez se tenga debidamente documentado el análisis de riesgos, se realizará y documentará la prueba piloto del sistema de acceso y autenticación que permita tener una gestión de identidad. En conjunto el proyecto se realizará en un plazo de 4 meses. Por último, lo que se busca es ayudar a la empresa Kappa10 a cumplir con los requisitos que le faltan para la obtención de la certificación ISO 27001 en el presente año, a saber 2018.

---

http://bibliotecavirtual.unad.edu.co:2051/login.aspx?direct=true&db=e000xww&AN=847674&lang=es&site=eds-live

[3] FORTINET. FortiAuthenticator [2017]. [en línea] [citado el 16 de mayo, 2018]. Disponible en internet: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiAuthenticator.pdf

[4] FORTINET. Access Management and Single Sign-On [Administración de acceso e inicio único de sesión]. [2018]. [en línea] [citado el 16 de mayo, 2018]. Disponible en internet: https://www.fortinet.com/products/identity-access-management/fortiauthenticator.html

## INTRODUCCION

Los sistemas de gestión de seguridad de la información SGSI, por sus siglas en inglés, se han vuelto necesarios, y en muchos casos imprescindibles para el manejo de cualquier empresa que desee surgir y mantenerse vigente en el mercado. Parte de las labores de los SGSI es regular los riesgos que se presenten en cada uno de los activos tecnológicos de la empresa, para lo cual se usan diferentes metodologías que permiten tener información concreta que más adelante se utiliza en los análisis de riesgos. Esta gestión del riesgo, como se conoce comúnmente, permite a las empresas mantener un nivel de servicio acorde al mercado.

Normalmente la gestión de riesgos se hace mediante un análisis que permita identificar claramente la situación actual de la compañía, y permita además, cumplir con algún objetivo trazado, por ejemplo, obtener un certificado o sello de calidad de una entidad reconocida, implementar mejoras en su infraestructura tecnológica, o deshacerse de cargas innecesarias. Un análisis de riesgos bien hecho permite a las directivas determinar cómo es, cuánto vale, y cuanta protección tiene el sistema, lo que facilitará la toma de decisiones basadas en hechos, que sean coherentes y estén dirigidas al cumplimiento de objetivos.

Uno de los objetivos que más persiguen las entidades prestadoras de servicios tecnológicos en Colombia al realizar un análisis de riesgos, es poder obtener la certificación ISO 27001, ya que es una garantía de buen servicio para clientes actuales y futuros.

A lo largo del proyecto se presentan los diferentes ámbitos del análisis de riesgos dentro de una empresa, que van desde el reconocimiento e inventariado de sus activos de infraestructura tecnológica, hasta el plan de tratamiento de los riesgos identificados durante el proceso. Este análisis se considera un punto de partida para el ciclo de mejora continua, y la base para que la empresa pueda ofrecer sus servicios y crecer de forma ordenada. Durante las fases del proyecto se aplicará MAGERIT, una metodología de análisis de riesgos aprendida durante la

especialización, poniendo en práctica el conocimiento y herramientas previamente brindadas por la universidad.

El alcance del proyecto comprende el cumplimiento del análisis de riesgos de la infraestructura tecnológica de la empresa, así como la prueba piloto del sistema de gestión de identidad. La línea de investigación a la cual se aplica el proyecto es la de Infraestructura tecnológica y seguridad en redes.

# 1 PROBLEMA DE INVESTIGACIÓN

La compañía Kappa10 Ltda.[5] es una empresa dedicada a la venta de servicios y equipos de seguridad informática, *partner* de una de las empresas de seguridad líder en el mundo informático actual, como es la marca Fortinet[6]. La empresa cuenta con varios usuarios tanto de la parte administrativa como de la parte operativa, los cuales son controlados mediante directorio activo de Windows.

La parte operativa se divide en dos secciones, implementación y soporte, pero actualmente ninguna cuenta con una buena gestión de identidad a la hora de realizar configuraciones y cambios en los equipos de seguridad administrados y soportados por la compañía, ya que todos los ingenieros utilizan el mismo usuario y contraseña genéricos para estos fines, lo que supone un riesgo a la hora de llevar el control de cambios.

Para dar un ejemplo estadístico de la problemática, el mes de febrero de 2018, el área operativa atendió un promedio de 13 requerimientos de cliente externo al mes por ingeniero (Sin tener en cuenta reuniones, documentación, correo, requerimientos internos, etc.), se atendieron un total de 27 clientes entre los 4 ingenieros del área[7].

En promedio, cada cliente maneja 2 equipos de seguridad informática, lo que sería un aproximado de 54 dispositivos, que finalmente se traducen en por lo menos 432 eventos de *logon* (aparte de los eventos de *logoff*) y cambios realizados, si se maneja un estándar de 8 cambios realizados por equipo para dar solución a cada requerimiento (que pueden ser creación, modificación y eliminación de políticas de firewall, de perfiles UTM, de enrutamiento, etc.) Esto genera dificultad de

[5] KEY APPLICATION ASSURANCE LEVEL TEN LTDA. Kappa 10 ltda. [2018]. [en línea] [citado el 25 de octubre, 2018]. Disponible en internet: http://www.kappa10.com/
[6] FORTINET INC. [2018]. [en línea] [citado el 25 de octubre, 2018]. Disponible en internet: https://www.fortinet.com/
[7] Estadística obtenida del software de información iTop de Kappa10 Ltda.

seguimiento de cambios, que incluso a la fecha no son totalmente documentados en la herramienta, volviendo más ardua la tarea de administración de los equipos.

El problema como tal se ubica en la línea de investigación de infraestructura tecnológica y seguridad en redes, ya que hace referencia a cubrir la necesidad que surge a raíz de la búsqueda de la certificación de la empresa en ISO 27001. El proyecto busca desarrollar la temática del análisis de riesgos de la empresa Kappa10 Ltda. de donde se desprenderán las acciones a tomar para implementar los controles de mitigación de estos.

En el marco de referencia del proyecto, en lo que respecta a infraestructura de seguridad, los clientes del área operativa funcionan de forma muy similar a la empresa en cuestión, ya que todos tienen equipos de seguridad informática de la marca Fortinet, los cuales ayudan a prevenir los riesgos a nivel perimetral.

La oficina principal de Kappa10 Ltda. cuenta con un firewall de siguiente generación (NGFW) modelo FortiWiFi 60D-POE[8], y la oficina secundaria tiene un firewall de siguiente generación modelo FortiGate 60D[9]. Estos equipos controlan el flujo de datos internos entre las dos oficinas por medio de una VPN *Site-to-Site*, y controlan el tráfico hacia internet de los usuarios por medio de características de filtrado de URLs y de aplicaciones.

Teniendo como escenario la infraestructura descrita anteriormente, se tiene una empresa con una base de datos de alrededor de 40 clientes con infraestructuras de red similares, de los cuales administra cerca de 70 Firewalls, y algunos equipos de análisis de logs de la marca Fortinet. Como se mencionó previamente, todos los equipos se administran con el mismo usuario y clave, ya que no se cuenta con una adecuada gestión de identidad que permita tener un control de cambios efectivo y acorde a todas las buenas prácticas de ITIL[10].

[8] FORTINET. FortiGate/FortiWiFi 60D Series [2016]. [en línea] [citado el 16 de mayo, 2018]. Disponible en internet: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_FortiWiFi_60D_Series.pdf

[9] Ibíd.

[10] IT PRENEURS Y AXELOS. Curso ITIL Foundation. Release 3.3.1. [2014]. Bogotá: 2013. 457p.

Es conocido que el principal problema de Kappa10 radica en usar únicamente un usuario y contraseña para acceder a los dispositivos de seguridad administrados, lo que genera varios riesgos de seguridad que deben ser mitigados para que la empresa aspire a certificarse en ISO 27001[11].

Algunos de los riesgos son cosas como, no tener el control de quien hizo un cambio, cuando lo hizo, porque lo hizo, fraudes de identidad, un incorrecto descargo de responsabilidades, entre otras. Lo anterior causa anomalías en los servicios prestados, y al no tener ninguna trazabilidad, se generan reprocesos, demoras en la solución, desconocimientos y en general inconformidad por parte de los clientes. En resumen, a simple vista resaltan algunos riesgos, y de acuerdo con un análisis de riesgos previo realizado por el área de conformidad de la empresa, puntualmente en el primer semestre del 2018, aún hay más riesgos latentes por detectar con miras a crear un entorno tecnológico seguro que permita a la empresa cumplir con sus metas de certificación y posicionamiento en el mercado.

## 1.1 FORMULACION DEL PROBLEMA

¿Cuáles son los riesgos de seguridad de la información que la empresa Kappa10 debe mitigar para adquirir la certificación ISO 27001:2013 en el año 2019?

[11] ICONTEC. Norma técnica ntc iso/iec colombiana 27001 [2006]. [en línea] [citado el 16 de mayo, 2018]. Disponible en internet: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

# 2 OBJETIVOS

## 2.1 OBJETIVO GENERAL

Analizar los riesgos de seguridad de la información de la infraestructura tecnológica de la empresa Kappa10 limitada y generar las recomendaciones que permitan que la empresa haga los respectivos ajustes encaminados a obtener la certificación ISO 27001:2013.

## 2.2 OBJETIVOS ESPECÍFICOS

- ✓ Realizar el inventario de activos de infraestructura tecnológica de la empresa Kappa10.
- ✓ Analizar los riesgos de seguridad de la información de cada uno de los activos de infraestructura tecnológica de la empresa Kappa10.
- ✓ Proponer un plan de tratamiento para cada riesgo de nivel inaceptable detectado durante el análisis de riesgos de seguridad de la información.
- ✓ Recomendar las posibles acciones de seguridad de la información a emprender para la empresa Kappa10.
- ✓ Evaluar la mitigación de los riesgos de gestión de identidad de la empresa mediante la prueba piloto de autenticación.

# 3 JUSTIFICACIÓN

Kappa 10 es una empresa prestadora de servicios de seguridad informática, y como tal, es necesario que periódicamente realice un análisis de riegos de seguridad de la información con el fin de detectar áreas de mejora, con miras a cumplir los requisitos de certificación y los estándares de servicio del mercado. Este proyecto debe realizarse para generar una mayor calidad de servicio a los clientes de la empresa, creando un ambiente de confianza respaldado por la certificación ISO 27001[12], lo que a su vez contribuirá a que los potenciales nuevos clientes escojan la empresa por su preparación y fortaleza en el área de la seguridad informática.

La certificación mencionada es prenda de garantía para los clientes de Kappa10, ya que la distinguiría como una empresa organizada y responsable, digna de confianza y con procesos efectivos enfocados al logro, lo que sin duda ayudará a mantener los clientes actuales y a conseguir nuevos clientes, sobre todo en los casos en los que las licitaciones tienen esta certificación como uno de los requisitos del futuro proveedor, sobre todo en verticales de gobierno, salud y servicios de tecnología.

Otro tema que entra en consideración a la hora de querer alinear los procesos y servicios de Kappa10 de acuerdo con las normas ISO 27001, es el crecimiento ordenado de las áreas, ya que esta es una empresa pequeña, pero con grandes horizontes de crecimiento, y es de esperar que al crecer aparezcan nuevos roles y más servicios, que pueden jugar en contra si no se mantienen controlados y documentados en el SGSI.

Finalmente, el tercer motivo por el cual se debe realizar este análisis de riesgos en Kappa10, es corregir y mitigar riesgos notorios, como el de no tener una correcta gestión de identidad en los dispositivos que maneja la empresa, o los riesgos intrínsecos que este conlleva, como el fraude y la suplantación, por lo cual el proyecto plantea documentar los riesgos de los activos de infraestructura

[12] ICONTEC. Op. Cit., p. 26.

tecnológica de la empresa de acuerdo con las normas ISO 27001 y la metodología MAGERIT[13] versión 3.

El proyecto plantea hacer algo que ya se ha realizado previamente en muchas entidades, sin embargo, como ninguna compañía es igual a otra, es necesario que la norma se aplique de acuerdo con la medida de cada una, y es por eso que en Kappa10 Ltda. es necesario llegar a una aplicación de la misma para lograr un análisis de riesgos completo y acertado, que permita tomar las mejores decisiones a la junta directiva.

El proyecto además busca desarrollar la temática del análisis de riesgos de la empresa Kappa10 Ltda. con el fin de argumentar las recomendaciones que deberán implementarse dentro de esta para mitigar los riesgos inaceptables encontrados durante el periodo de revisión.

Posteriormente plantea una prueba piloto del sistema de autenticación tipo Enterprise[14] para Kappa10, con el propósito de mitigar del riesgo de no tener controles de identidad adecuados, los cuales se encuentran claramente definidos en el numeral A. 11 CONTROL DE ACCESO de la norma ISO 27001[15].

La prueba piloto manejará un servicio de logs, que al trabajar en conjunto con la gestión de identidad, permitirán llevar un registro de eventos de “logon” de los usuarios de ingeniería en los diferentes equipos de seguridad informática que se administran y soportan, tanto internamente como a nivel clientes. Finalmente, al evaluar los resultados del proyecto se espera obtener una documentación completa del análisis de riesgos y una propuesta de mitigación del riesgo evidente de gestión de identidad que sirvió como disparador de este.

---

[13] GOBIERNO DE ESPAÑA. MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro 1. [2012]. Madrid. [en línea] [citado el 20 de octubre, 2018]. Disponible en https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.W9NdSTFRepo

[14] BERNAL BUENO, Leonardo. Proyecto WPA2-Enterprise, Radius, LDAP [2013]. [en línea] [citado el 16 de mayo, 2018]. Disponible en internet: http://informatica.gonzalonazareno.org/proyectos/2012-13/lbb.pdf

[15] ICONTEC. Op. Cit., p. 26.

El desarrollo del proyecto contribuirá a que la empresa avance hacia la certificación ISO 27001, que cuente con la debida gestión de identidad, y que continué con la gestión documental necesaria para el SGSI y el cumplimiento de normas[16]. De esta manera se posicionará a Kappa 10 como una de las mejores empresas de prestación de servicios de seguridad informática de Colombia.

[16] FORTINET. Secure access solution [Solución de acceso seguro] [2017]. [en línea] [citado el 16 de mayo, 2018]. Disponible en internet: https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/SG-SAA-Enterprise-Network.pdf

# 4 MARCO DE REFERENCIA

## 4.1 MARCO TEÓRICO

La tecnología y las tendencias del mercado van cambiando de forma acelerada la manera en la que las empresas diseñan sus redes. Para habilitar nuevos negocios es necesario que las empresas prestadoras de servicios de ingeniería de seguridad informática cuenten cada vez con más y mejores herramientas que las hagan más competitivas en el mercado laboral colombiano, una de estas es la certificación ISO 27001[17], que describe cómo gestionar la seguridad de la información en una entidad.

Las normas ISO 27001 en su numeral 3.13 contempla que la seguridad de la información involucra propiedades tales como la autenticidad, la trazabilidad, el no repudio y la fiabilidad, por lo que se hace necesario identificar quien realiza cada movimiento en los activos tecnológicos de la compañía[18]. Por este y otros motivos, el proyecto contempla la revisión de este tipo de falencias mediante un análisis de riesgos metodológico.

Hay varias metodologías de análisis de riesgo que son conocidas hoy en día, y que ayudan a las empresas a mantener aceptable su nivel de riesgo informático. Para realizar un análisis de riesgos completo, es necesario conocer muy bien la infraestructura de la empresa, entender el corazón del negocio que maneja, y comenzar de manera ordenada a recolectar información, organizarla y analizarla, con el fin de identificar las amenazas, los riesgos, las causas, los controles utilizados, y en general todo lo concerniente a los activos de información de esta.

Hacer esto es cada vez más complejo por factores como el crecimiento desmedido de dispositivos de red en las empresas. Por esta razón los análisis de riesgos deben ser cada vez más exhaustivos, específicos, y encaminados a la revisión de procesos

[17] ICONTEC. Norma técnica ntc-iso/iec colombiana 27001. Op. cit. p. 34.
[18] KEY APPLICATION ASSURANCE LEVEL TEN LTDA. Kappa 10 ltda. Op. cit. p. 1.

y organización, como es el caso de la norma ISO 27001:2013[19], en la cual se plantea seguir un ciclo de mejora continua que pretende establecer el contexto del proceso, valorar su riesgo, y tratarlo con los controles requeridos con el fin de mitigarlo. Este ciclo se convierte en una constante, ya que, al ser cambiante la tecnología y sus medios, nuevos riesgos y vulnerabilidades irán saliendo día a día en cada proceso.

Una muestra de esto son los dispositivos BYOD[20] (Bring Your Own Device) como smartphones, tabletas, smartwatch, etc. Y el uso cada vez más creciente de IoT (Internet de las cosas)[21], lo que a su vez causa un ritmo acelerado en el crecimiento de equipos de red como firewalls, switches, puntos de acceso, enrutadores, etc. Llegar a controlar una infraestructura cada vez más grande puede ser un desafío enorme si no se tienen en consideración factores de control de acceso automatizados y fáciles de administrar, que permitan una mejor trazabilidad de los activos y una mayor fiabilidad de los administradores.

Esto implica riesgos de seguridad latentes en el manejo de la información y procesos de cualquier compañía, y uno de los más grandes identificables es la inadecuada o inexistente gestión de identidad. Algunas compañías realizan sus análisis de riesgos de acuerdo con diferentes metodologías y normas, y depende mucho del tipo de empresa y el enfoque cuál de estos se use, sin embargo, algunos de los más usados actualmente son ISO 31000[22] y MAGERIT[23] versión 3, ya que contemplan un amplio espectro de factores, como procesos, organización, activos, gestión ambiental, entre otros.

[19] ICONTEC. Op. Cit., p. 1.
[20] FORTINET. BYOD [en línea]. The Fortinet Cookbook. (2018), p. 1. [Consultado: 10 de 11 de 2018]. Disponible en Internet: https://cookbook.fortinet.com/glossary/byod/
[21] FORTINET. What is IoT? [en línea]. IoT Security. (2018). [Consultado: 16 de noviembre de 2018]. Disponible en Internet: https://www.fortinet.com/resources/cyberglossary/iot-security.html
[22] ICONTEC. Norma técnica ntc-iso/iec colombiana 31000 [2006]. [en línea] [citado el 16 de mayo, 2018]. Disponible en internet: https://sitios.ces.edu.co/Documentos/NTC-ISO31000_Gestion_del_riesgo.pdf
[23] GOBIERNO DE ESPAÑA. Op. Cit., p. 1.

Muchas empresas han venido implementando su análisis de riesgos con base en las normas ISO 27001 e ISO 31000, por ejemplo, la empresa mexicana DAMSA[24] Soluciones integrales en capital humano, que es una compañía dedicada a la gestión de recursos humanos como bolsa de empleos, vio la necesidad de realizar esta labor debido a que querían ser más preventivos a la hora de enfrentar los riesgos, es por eso que luego de realizar la auditoria interna decidieron comenzar a ofrecer el servicio de análisis de riesgos a empresas de manufactura y a empresas enfocadas a servicios, como es el caso de Kappa10 Ltda.

Esta metodología de análisis de riesgos considera que se debe monitorear constantemente a todos los procesos pertenecientes al área informática de la empresa, creando un ciclo de mejora continua basado en la prevención de los riesgos, que finalmente representan las posibilidades que hay de no poder cumplir con los objetivos de la empresa.

La metodología de ISO 31000 plantea un pensamiento basado en riesgos, es decir, que al realizar cualquier acción o proyecto se debe pensar en función del riesgo, como se puede ver afectada la compañía, que procesos deben ser cuidadosamente revisados con el fin de no entorpecer los objetivos de la empresa, quien o quienes serán los responsables directos en cada proceso, y finalmente, que todos los colaboradores lleguen a la comprensión perfecta de este modelo y se conviertan a sí mismos en facilitadores de los procesos y manejadores del riesgo.

Lo anterior pone las bases para un esquema preventivo ante las amenazas, ya que permite detectar las fallas antes que ocurran, y si ocurren, permite atacarlas y mitigarlas con un tiempo de respuesta mucho menor al que se tendría sin un modelo de análisis de riesgos.

Otra empresa a la cual se le realizó este análisis basado en la norma ISO 31000:2009 fue al Grupo Alcomex[25], una empresa colombiana situada en la ciudad

[24] DAMSA. DAMSA Soluciones integrales en capital humano [en línea]. DAMSA. México (2018). [Consultado: 17 de noviembre de 2018]. Disponible en Internet: https://www.damsa.com.mx/

[25] GUTIÉRREZ CONEO, Jesús y PINEDA ARIAS, Juan. Análisis de riesgos de seguridad y salud por procesos basado en la norma ISO 31000:2011 para el Grupo Alcomex. Bogotá, 2016, 57p.

de Bogotá, dedicada al almacenamiento y transporte internacional de mercancías, a la cual los estudiantes de Ingeniería de producción de la Universidad Distrital Francisco José de Caldas, llamados Jesús Gutiérrez, y Juan Pineda, realizaron un completo análisis de riesgos basados en los procesos de esta, el cual pueden consultar en el enlace citado más adelante en la bibliografía.

Así como estas empresas, hay muchas otras a las cuales se les ha realizado el análisis de riesgos con base en la norma ISO 31000, por ejemplo, algunas de ellas son el cliente TGE de la Empresa Assurance Controltech[26], de acuerdo a la tesis de Ingeniería de Sistemas de la señora Diana Jara, también de la Universidad Distrital Francisco José de Caldas, el organismo nacional de acreditación ONAC[27], como lo indica el trabajo de grado de ingeniería industrial de la Universidad Javeriana de los señores Juan Garavito, David Palomares y Jhorman Santamaría, entre muchos otros.

De acuerdo con el enfoque de la segunda parte del trabajo, se habla del riesgo que actualmente tiene la gestión de identidad dentro de los procesos de la empresa. La gestión de identidad es un área administrativa extensa que se encarga de la identificación de individuos en un sistema, como un país, una red, una empresa, etc. y también de controlar su acceso a los recursos dentro de ese sistema por medio de la asociación de los derechos y restricciones de usuario de acuerdo con la identidad establecida[28].

---

Trabajo de grado (Ingeniería de Producción). Universidad Distrital Francisco José de Caldas. Facultad de Tecnología.

[26] JARA PÉREZ, Diana. Valoración y plan de tratamiento de riesgos de seguridad de la información para los procesos incluidos en el alcance del SGSI del cliente TGE de la empresa Assurance Controltech. Bogotá, 2017, 58p. Trabajo de grado (Ingeniería de Sistemas). Universidad Distrital Francisco José de Caldas. Facultad de Ingeniería.

[27] GARAVITO ARENAS, Juan, PALOMARES GUTIÉRREZ, David y SANTAMARÍA ORJUELA, Jhorman. Diseño de una metodología de planeación y monitoreo de los procesos clave del Organismo Nacional de Acreditación para una proyección internacional de la acreditación. Bogotá, 2015, 270p. Trabajo de grado (Ingeniería Industrial). Pontificia Universidad Javeriana. Facultad de Ingeniería.

[28] ROUSE, Margaret. Gestión de identidades, ID management. [2016]. [en línea] [citado el 16 de mayo, 2018]. Disponible en internet: https://searchdatacenter.techtarget.com/es/definicion/Gestion-de-identidades-ID-management

Parte importante del sistema de gestión de identidad es la tecnología que lo soporta y brinda ese nivel de confiabilidad de los recursos, por eso, más adelante veremos la forma en la que actualmente algunas empresas realizan el manejo de la tecnología de control de accesos.

A nivel internacional es normal que la mayoría de las empresas grandes ya cuenten con sistemas de autenticación tipo Enterprise, un caso cercano es el de la empresa de comunicaciones Claro, que a nivel Colombia cuenta con sistemas de autenticación Enterprise basados en TACACS+[29], RADIUS[30] y LDAP[31] para diferentes tipos de servicios y dependiendo del área en el cual se van a usar. Por ejemplo, en el área de seguridad informática, encargada de administrar los dispositivos Firewall a nivel perimetral e interno, cuenta con autenticación Enterprise TACACS+ en sus equipos de las marcas Fortinet, Cisco y Checkpoint.

La autenticación Enterprise es muy popular en países más desarrollados, como Estados Unidos y los del continente europeo, en donde la mayoría de las empresas grandes cuenta con un modelo de seguridad sofisticado por capas, que incluye:

Capa de administración: Donde se encuentran los equipos de manejo y monitoreo de los dispositivos de red (Single pane of glass). En esta capa están los encargados de verificar el estado de la red y sus componentes, así como de reportar las anomalías que ocurran en estos y tomar alguna acción si es necesario.

Capa de Seguridad y Control: Donde se encuentran los equipos de seguridad tales como NGFW (Firewalls de siguiente generación[32]), ISFW (Firewalls de

[29] ROUSE, Margaret. TACACS (Terminal Access Controller Access Control System). [2007]. [en línea] [citado el 15 de diciembre, 2018]. Disponible en internet: https://searchsecurity.techtarget.com/definition/TACACS

[30] --------. RADIUS (Remote Authentication Dial-In User Service). [2007]. [en línea] [citado el 15 de diciembre, 2018]. Disponible en internet: https://searchsecurity.techtarget.com/definition/RADIUS

[31] --------. LDAP (Lightweight Directory Access Protocol). [2007]. [en línea] [citado el 15 de diciembre, 2018]. Disponible en internet: https://searchmobilecomputing.techtarget.com/definition/LDAP

[32] FORTINET. Next-Generation Firewall [Firewall de siguiente generación] [2018]. [en línea] [citado el 16 de mayo, 2018]. Disponible en internet: https://www.fortinet.com/products/next-generation-firewall.html

segmentación interna), los DCFW (Firewalls de centros de datos) y los DEFW (Firewall de oficinas distribuidas).

Capa de acceso: Donde se manejan los dispositivos de red como puntos de acceso, switches capa 2 y capa 3, para que se conecten los usuarios finales o los servidores. En esta capa no se encuentran usuarios ni hosts finales, ya que únicamente se encarga de proporcionar el medio de conexión para estos.

Capa de Clientes: Donde se encuentran los equipos de usuario final, como computadoras, laptops, servidores, tabletas, smartphones, smartwatch, etc. Es una de las capas más importantes del modelo, ya que es donde se encuentran los usuarios que finalmente generarán los eventos de autenticación.

Adicionalmente, este modelo plantea una capa transversal de acceso seguro, la cual consiste en el manejo de identidad mediante un directorio activo, y en algunos casos factores de doble o triple autenticación dependiendo del nivel de seguridad requerido.

***Parámetros de autenticación Enterprise***

Para el manejo de un ambiente de acceso seguro es necesario contar con varios controles de identidad de los usuarios, que sean confiables y tengan trazabilidad. Por lo tanto, es preciso tener un servidor donde se registren los eventos de “login” de los usuarios, y además de esto un servicio de autenticación fuerte que pueda engranar con el servidor. Con estos dos elementos se puede tener una autenticación controlada, pero también es de suma importancia mantener un registro de logs de los eventos generados para lograr una trazabilidad completa.

Los dispositivos que se van a utilizar son:

- Servidor de directorio activo de Windows: Es una herramienta de Microsoft para realizar la organización y gestión de una red de ordenadores y todo lo que implica, como el manejo de usuarios, servicios, puestos, impresoras, permisos,

servidores, etc. Allí es donde se almacena la información de todos los componentes de la red, lo que permite al administrador tener un único punto de gestión de esta. El directorio activo ayuda al administrador a gestionar los usuarios por grupos de forma ordenada, por ejemplo, comercial, administrativo, soporte, y otros varios. Este funciona como un almacén de contraseñas, ya que es el lugar a donde van los eventos de inicio y cierre de sesión del sistema operativo de los PC de la red[33].

- FortiAuthenticator[34] VM: Es un dispositivo encargado de administrar la identidad de usuarios de una empresa de forma segura por medio de simplificar y centralizar el manejo y repositorio de la información de los usuarios. Puede funcionar como Hardware o máquina virtual, dependiendo de las necesidades y el entorno de red de la empresa, en el proyecto se plantea usar su forma virtual. su trabajo es habilitar un acceso de red controlado y seguro a cada usuario de acuerdo con su rol, para lo cual se integra de forma transparente con el LDAP o el directorio activo de Windows, sin generar carga a los usuarios al tener que autenticarse más de una vez. Puede integrarse con su entorno de varias maneras, como:
  - Haciendo Polling de los eventos del directorio activo.
  - Integrando Single-Sign-On (SSO) con un agente instalado en el servidor de directorio activo, el cual le ayuda a detectar los eventos de login, los cambios de IP. y los eventos de logout.
  - Haciendo SSO de autenticación basado en portal.
  - Monitoreando los logs de inicio de un RADIUS.

[33] MARTINEZ ALEGRE, Francisco. ¿Qué es el directorio activo de Microsoft? [2013]. [en línea] [citado el 16 de mayo, 2018]. Disponible en internet: http://www.martinezalegre.com/2011/03/que-es-el-directorio-activo-de-microsoft/

[34] FORTINET. FortiAuthenticator [2017]. [en línea] [citado el 16 de mayo, 2018]. Disponible en internet: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiAuthenticator.pdf

Sus principales características y beneficios son:

- ✓ Identificación transparente de los usuarios sin impacto operativo para la empresa.
- ✓ Integración con LDAP y AD para realizar identificación por grupos de usuarios, reduciendo el tiempo de implementación de la plataforma.
- ✓ Un rango amplio de opciones de identificación de usuarios, con flexibilidad para integrarse con cualquier entorno empresarial.
- ✓ Permite habilitar seguridad basada en roles, dando un mayor control al administrador de la plataforma.

El dispositivo cuenta además con algunas características adicionales que se pueden usar en el proyecto, como:

- ✓ Autenticación con LDAP y RADIUS, que crea una base de datos local y centraliza la administración de usuarios.
- ✓ Métodos de autenticación fuerte, con token, correo, SMS, y certificados digitales, que pueden evitar ataques de fuerza bruta efectivos.
- ✓ Recuperación de claves de usuario sin intervención del administrador.
- ✓ Integración con LDAP y AD existentes, lo que mejora los tiempos de implementación y además reutiliza el entorno actual.

Los hipervisores que soportan la máquina virtual son: VMware ESXi / ESX 3.5 / 4.0 / 4.1 / 5.0 / 5.5 / 6.0, Microsoft Hyper-V Server 2008 R2, 2012, y 2012 R2, KVM.

La capacidad de la máquina virtual depende de la licencia aplicada.

- ➢ FortiGate: Es un dispositivo de seguridad que contiene todo el manejo unificado de amenazas (UTM); cortafuegos, IPS, control de aplicaciones, VPN, filtrado web y el controlador inalámbrico integrado. Además, incluye la última tecnología de protección avanzada de antivirus, diseñada para generar una defensa contra

amenazas avanzadas persistentes (APT), lo que lo convierte en una solución NGFW. Ofrece un buen rendimiento de firewall de acuerdo con su modelo, ya que puede servir para empresas pequeñas u hogares hasta grandes Carriers de comunicaciones.

Puede presentarse en Hardware o como máquina virtual[35], donde es compatible con los hipervisores descritos en la tabla 1 “Hipervisores compatibles con FortiGate”:

Tabla 1 Hipervisores compatibles con FortiGate.

| Tipo de ambiente del hipervisor | Versiones del hipervisor compatibles |
|---|---|
| Nube privada | ➢ VMware ESXi v5.0 / v5.1 / v5.5 / v6.0 / v6.5<br>➢ Microsoft Hyper-V Server 2008 R2 / 2012 / 2012 R2 / 2016<br>➢ Citrix Xen XenServer v5.6 sp2, v6.0, v6.2 and later<br>➢ Open source Xen v3.4.3, v4.1 and later<br>➢ KVM qemu 0.12.1 & libvirt 0.10.2 y posteriores, y para red hat Enterprise Linux / CentOS 6.4 and later / Ubuntu 16.04 LTS (generic kernel) |
| Nube pública | ➢ Amazon AWS (Amazon Web Services)<br>➢ VMware Cloud on AWS<br>➢ Microsoft Azure<br>➢ Google GCP (Google Cloud Platform)<br>➢ Oracle OPC (Oracle Public Cloud) |

Actualmente estos dispositivos ejecutan un sistema operativo de fabricante llamado FortiOS, que se encuentra en la versión 5, el cual ofrece una mayor seguridad para combatir amenazas avanzadas, un mayor control y seguridad para dispositivos móviles, y una mayor inteligencia para construcción de políticas de seguridad sin generar más carga operativa.

La mayoría de los clientes de Kappa10 cuentan con uno o más de estos Firewalls de nueva generación, administrados y soportados por el área de ingeniería de la empresa.

[35] FORTINET. FortiGate Virtual Appliances [Dispositivos virtuales FortiGate] [2017]. [en línea] [citado el 16 de mayo, 2018]. Disponible en internet: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_VM.pdf

- FortiAnalyzer VM: Es una plataforma de centralización de logs y reportes que permite a los administradores de TI identificar rápidamente los problemas y amenazas de la red y poder tomar acciones preventivas y correctivas. Cuenta con un sistema operativo propio de Fortinet, desarrollado a la medida, y que permite integración con los dispositivos de la marca y con otras formas de logs más genéricas, como syslog.

  Al ser una máquina virtual[36] es escalable y flexible, soportando eventos de varios clientes a la vez, su capacidad depende del tipo de licencia y el hardware donde esté operando.

  Sus principales características son:

  - FortiView: un poderoso sistema de visibilidad de eventos de red, que es personalizable a la medida de cada cliente. Cuenta con graficas interactivas que permiten a los administradores enterarse de los eventos en segundos, además provee soluciones de monitoreo fáciles e intuitivas.
  - Indicadores de compromiso (IOC) que muestran los usuarios que son sospechosos de acuerdo con su actividad web.
  - Multi alquiler, lo cual permite tener diferentes clientes en dominios administrativos apartados y asignando diferentes cuotas de manejo dependiendo de las necesidades de cada cliente.
  - Reportería personalizada, que permite una mayor visibilidad y entendimiento del entorno de red. Los reportes se pueden programar o ser generados por demanda.
  - Monitoreo y alertas, que permiten configurar el sistema para enviar alertas de ciertos eventos vía email, comunidad SNMP, o Syslog.

[36] FORTINET. FortiAnalyzer Virtual Appliances [Dispositivos virtuales FortiAnalyzer]. [2018]. [en línea] [citado el 16 de mayo, 2018]. Disponible en internet: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiAnalyzer.pdf

- Modos de Centro de operaciones de red (NOC) y modo de Centro de operaciones de seguridad (SOC)
- Búsqueda de logs para análisis forense.

Proyectos similares:

- Proyecto WPA2-Enterprise, Radius, LDAP, enfocado a la implementación de autenticación Enterprise en ambientes Wireless[37].
- En España, Desarrollo de una intranet con Liferay (Intranet development with Liferay), Intranet con un sistema de autenticación de usuarios tipo enterprise con integración de varias plataformas[38].

Y así como estos ejemplos hay muchos en todo el mundo porque la autenticación con trazabilidad y control es una idea esencial en los procesos de seguridad de TI, para hacer de estos una forma segura de administrar una red y mantener controlados los cambios de esta.

## 4.2 MARCO CONCEPTUAL

Un análisis de riesgos es un proceso lógico y ordenado mediante el cual se estiman los niveles de riesgo a los que está expuesta una entidad. Hay varias metodologías de análisis de riesgos, que dependiendo de cada caso particular se encargan de

[37] BERNAL BUENO. Op. Cit., p. 6.
[38] GARCÍA TAMAYO, Rubén. Desarrollo de una intranet con Liferay (Intranet development with Liferay) [2011]. [en línea] [citado el 16 de mayo, 2018]. Disponible en internet: https://upcommons.upc.edu/bitstream/handle/2099.1/11785/PFC_GMV_Ruben_Garcia_Tamayo.pdf

plantear, organizar y poner en marcha el mejor sistema posible para mitigar o eliminar los riesgos de la entidad.

Algunas de las metodologías más usadas en la actualidad, son MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), OCTAVE (*Operationally Critical Threat, Asset, and Vulnerability Evaluation*), CRAMM (*CCTA Risk Analysis and Management Method*), MEHARI (Método Armonizado de Análisis de Riesgos), SP800-30 (*National Institute of Standards and Technology*), CORAS (*Construct a Platform for Risk Analysis of Security Critical Systems*) y EBIOS (Expresión de las necesidades e identificación de los objetivos de seguridad) [39].

#### 4.2.1.1 Metodología de análisis de riesgos

Para este caso se escogió la metodología MAGERIT por ser una de las más usadas para realizar el análisis y gestión de riesgos, es abierta, y esto permite que se adapte a cualquier campo. Fue creada por el Ministerio de Administraciones Públicas de España, y se ofrece como marco y guía para la administración pública. Debido a su carácter abierto, también es utilizada por entidades gubernamentales, además de grandes y pequeñas empresas en el sector privado.

La metodología MAGERIT busca conseguir los siguientes objetivos:

- Lograr que los responsables de los sistemas de información sean conscientes de que existen riesgos y es necesario tratarlos a tiempo [40].
- Ofrecer un método organizado, lógico y sistemático que permita realizar el análisis de riesgos de los sistemas de información.

[39] ALEMÁN NOVOA, Helena; RODRIGUEZ BARRERA, Claudia. Metodologías para el Análisis de Riesgos en los SGSI. [2015]. [en línea] [citado el 15 de diciembre, 2018]. Disponible en internet: http://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1874
[40] Ibíd.

- Apoyar en la descripción y planificación de las medidas más acertadas para mantener los riesgos descubiertos bajo control.
- Disponer a la organización para los procesos de auditoría, evaluación, acreditación o certificación, según corresponda en cada caso. Por ejemplo en Colombia las empresas enfocadas a servicios tecnológicos pueden encaminarse a conseguir la certificación ISO 27001.

Al aplicar la metodología MAGERIT y enfocarla en los objetivos planteados, es posible llegar a determinar la situación de riesgo en la que se encuentra un activo informático, y establecer las acciones que se deben tomar para controlarlo y/o mitigarlo.

Por lo general, estos análisis se adhieren a los pilares fundamentales de la seguridad de la información, a saber, disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad. Estas dimensiones de seguridad son las sugeridas por MGERIT para evaluar y gestionar el riesgo, ayudando a determinar los principales activos de infraestructura tecnológica mediante un levantamiento de información que muestra los servicios soportados, su relación en la entidad, su valor, etc. Al aplicar MAGERIT para realizar la caracterización y valoración cuantitativa de los activos, es más fácil llegar a reconocer las vulnerabilidades y amenazas a las que están expuestos.

Durante todo el proyecto se hablará del riesgo, que es la medida de exposición a que una amenaza se haga real sobre uno o más activos tecnológicos causándole algún daño o perjuicio a la entidad[41]. Este concepto indica que es lo que puede llegar a pasar a un activo si no es protegido adecuadamente con las salvaguardas necesarias.

[41] GOBIERNO DE ESPAÑA. MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro 1. [2012]. Madrid. [en línea] [citado el 20 de octubre, 2018]. P. 127. Disponible en internet: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.W9NdSTFRepo. p. 9.

El análisis de riesgos es un proceso ordenado y estructurado que permite estimar la magnitud de los riesgos a los que se expone una organización[42]. El análisis de riesgos brinda un modelo del sistema en términos de activos, amenazas y controles[43]. Este análisis de riesgo permite determinar la forma del activo (por ejemplo si son datos, *hardware* o *software*), su valor y cuál es su nivel actual de protección. Una vez se identifican estas cosas, se analizan los riesgos y se plantea el plan de tratamiento de riesgos para poder mitigarlos.

Por otro lado, la gestión de riesgos es sencillamente la parte del proceso en la cual se eligen e implementan los controles o salvaguardas que permiten conocer, prevenir, impedir, reducir o controlar los riesgos registrados[44]. La gestión de riesgos es la estructuración de las acciones de seguridad que se ejercen para poder satisfacer las necesidades de control detectadas durante el análisis.

#### 4.2.1.2 Selección de activos

Los activos son los recursos de un sistema de información o que se encuentran en relación con este, que necesita una organización para poder funcionar de forma correcta y así poder alcanzar sus objetivos propuestos[45]. Es importante identificar al responsable de cada activo, establecer las relaciones entre activos, ubicar la dimensión de relevancia y valorar está en función de su importancia. En la selección de activos se deben considerar las siguientes características, como su dependencia, su valoración, y su coste, explicadas a continuación.

Los activos forman árboles de dependencias, los que estén arriba, superiores, en la estructura, dependen de los activos inferiores. Así es como se generan las

[42] Ibíd., p. 6.
[43] Ibíd., p. 6.
[44] Ibíd., p. 8.
[45] Ibíd., p. 22.

dependencias, de arriba hacia abajo, mientras que las amenazas se generan de abajo hacia arriba.

La valoración de los activos se clasifica de acuerdo con su valía para la empresa. Estos pueden ser críticos, importantes, medios o bajos dependiendo de sus características y roles. Por ejemplo, los activos críticos son aquellos imprescindibles para el sistema, y son los que imperativamente se deben proteger, por esta razón, cuanto más importante es un activo, mayor es el nivel de protección que requiere.

Como se explicó anteriormente, hablando de las dimensiones un activo puede tener varias. Las más importantes son las contenidas en la sigla CIDAT (Confidencialidad, Integridad, Disponibilidad, Autenticidad, y Trazabilidad), ya que es mediante la valoración de cada una de estas que el activo recibe su valor cualitativo y cuantitativo.

En detalle, la confidencialidad es la que asegura que la información llegue únicamente a las personas que están autorizadas para verla. La confidencialidad de la información puede ser vulnerable a cosas como las fugas de información y los accesos no autorizados. Una vez vulnerada, la confidencialidad es una característica difícil de recuperar, ya que mina la confianza de dentro y fuera de la organización[46].

La Integridad implica mantener las características de completitud y corrección de los datos. Asegurar que la información no ha sido alterada en el proceso de manejo, porque esto afectaría directamente al correcto desempeño de las funciones de una entidad[47].

La disponibilidad es la disposición de la información a ser usada cuando sea requerida[48]. Si no hay disponibilidad, los procesos y servicios que necesitan de la

[46] INFOSEGUR. Objetivos de la seguridad informática. [2013]. [en línea] [citado el 16 de mayo, 2018]. Disponible en internet: https://infosegur.wordpress.com/tag/confidencialidad
[47] Ibíd.
[48] Ibíd.

información se verán truncados, lo que afectará enormemente la imagen de la compañía.

La autenticidad implica una responsabilidad en el procesamiento de la información, ya que es la que permite al responsable saber con exactitud los procedimientos y formas de ingreso de datos utilizadas. Si no se cuenta con procedimientos de seguridad adecuados, la entidad se expone a la suplantación de identidad.

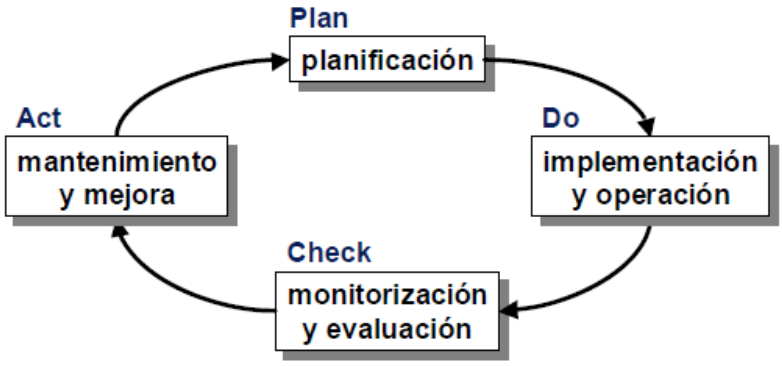
La trazabilidad es la que asegura un seguimiento permanente del activo. Por medio de esta se determina quién, cómo y en qué momento realizó ajustes, cambios o modificaciones a la información. La trazabilidad es esencial para el análisis de incidentes, el rastreo de atacantes y el aprendizaje de la experiencia. Esta se hace tangible en cosas como los registros de actividad de los activos de información.

Ahora bien, la valoración del coste del activo es la determinación del costo monetario o de operación que supondría recuperarse de una incidencia que destruyera el activo. Esta puede ser cualitativa, o sea, que muestra el valor que tiene cada activo en un orden relativo respecto de los demás, o cuantitativa, que permite asignar y operar valores numéricos de cada activo. Por ejemplo, si la valoración es monetaria, se puede hacer un estudio económico.

### 4.2.2 SGSI

Un SGSI (Sistema de Gestión de la Seguridad de la Información) puede definirse como la organización que nace para gestionar los procesos que están relacionados con la seguridad de la información. Normalmente, los SGSI se ajustan al ciclo Deming (PDCA) con el propósito de mantener y mejorar la calidad de sus servicios y productos.

Figura 1. Ciclo Deming o PDCA.




Fuente: MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro 1. P. 114.

Cada acción de estas se hace en pro de mantener y mejorar los procesos de la entidad, y por ende en cada paso se realizan diferentes actividades. Al planificar (P - Plan) se fijan los objetivos y se hacen los planes para alcanzarlos. Previamente debe tenerse el estado actual de la organización, esto es necesario para identificar en qué punto se está y para donde se quiere ir.

En la fase de hacer (D - Do) se ejecutan los planes y todas las acciones que estos implican. Al verificar (C - Check) se evalúan los resultados obtenidos de la anterior fase para determinar hasta qué punto se han concretado los objetivos. Finalmente, en la fase actuar (A - Act), y de acuerdo con la mentalidad de la mejora continua, en esta fase se actualizan los planes para enfocarlos a cumplir lo que falte de los objetivos, y se vuelve a iniciar el ciclo para que se pueda brindar un servicio cada vez mejor.

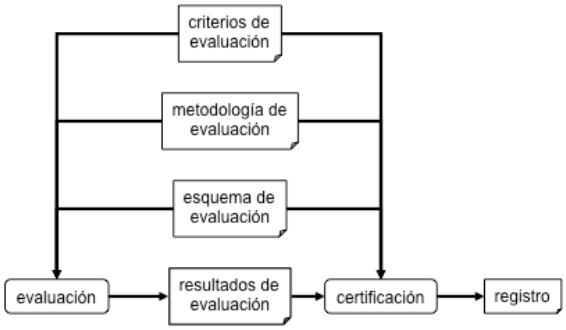
La evaluación de un SGSI depende de la madurez que tenga cada uno de los pasos del ciclo PDCA, y sobre todo de la documentación de los procesos y el cumplimiento de estos, ya que procedimientos que se encuentran solo en la mente de los empleados no se pueden considerar como algo maduro.

Los SGSI nacen enfocados a conseguir distintas metas de organización, entre las cuales está la certificación, que es realizada por un ente externo. El caso que atañe a este proyecto es la certificación ISO 27001:2013. El ente que certifica compromete

por escrito su palabra y credibilidad en ello, por lo que no son procesos tomados a la ligera, de tal forma que todo lo concerniente a procesos, servicios y activos de la información, debe estar normalizado y documentado de manera coherente y comprensible.

Para poder obtener una certificación de este tipo, la entidad debe cumplir con unos requisitos muy específicos, los cuales son regidos por unos “Criterios Comunes” (CC) establecidos internacionalmente desde los años 90 por las normas de comercio internacional. Estos CC permiten definir las funciones de seguridad de los productos y sistemas, y ayudan a determinar cómo evaluar la calidad de estos. De acuerdo con estos CC, un SGSI puede ser certificado o no, siguiendo un ciclo que en la mayoría de los casos cumple las siguientes fases:

Figura 2. Proceso global de certificación de un SGSI.




Fuente: MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro 1. P. 118.

La imagen anterior deja ver que una vez la organización tenga listo y documentado su SGSI actual, puede pasar a solicitar la revisión de un evaluador, quien será el encargado de verificar si la entidad y su SGSI cumplen los requisitos necesarios para obtener el título al que aspiran dentro de los criterios comunes.

### 4.2.3 Autenticación tipo Enterprise.

Actualmente las redes no tienen un perímetro visible, como solían tener en tiempos pasados, por lo que ahora es imperativo hallar una forma de controlar quienes

acceden al activo más importante de la compañía, la información. De ahí nace la necesidad de contar con un sistema de políticas de gestión de identidad que sea simple, efectivo y a la vez robusto. El principal objetivo de una empresa es ofrecer a sus empleados acceso seguro y controlado a sus recursos en red, habilitando el acceso a la persona indicada, en el momento indicado y a la información indicada sin comprometer la seguridad.

Para eso se inventó la autenticación tipo Enterprise, la cual comprende cosas como el inicio de sesión simple (Single Sign On), el doble factor de identificación, y los permisos basados en roles. En las redes actuales es común encontrarse con varios tipos diferentes de autenticación para diferentes plataformas, por ejemplo, Directorio Activo de Windows, Radius, Tacacs+, e incluso uso de certificados para autenticación, por lo que se debe encontrar una herramienta que permita unificarlos y administrarlos de manera rápida y sencilla.

En general los sistemas SSO interceptan e interpretan los eventos de *logon* para poder ingresar a las demás plataformas o servicios usando estos de forma automatizada, sin que el usuario tenga que volver a digitar su clave en cada una de ellas, es por eso por lo que minimizan bloqueos de cuentas y maximizan el rendimiento de los usuarios.

Para este proyecto se ha escogido una plataforma que integra varios de los servicios de gestión de identidad necesarios para el buen funcionamiento de una compañía. FortiAuthenticator[49] es una herramienta dedicada exclusivamente a la gestión de identidad, por lo que integra plataformas como Windows AD, Radius, Tacacs+, Kerberos, autenticación multifactorial, entre otros, por lo que es ideal para cualquier entorno empresarial en el que se desee controlar a los usuarios desde un mismo dispositivo de forma sencilla. La herramienta es fácilmente escalable, es robusta y cuenta con varias formas de operación dependiendo de cada caso.

[49] FORTINET. FortiAuthenticator. Op. cit. p. 1.

Algunas de las razones por las cuales una empresa puede preferir esta solución sobre otras marcas, incluyen las descritas en la tabla 2 “Características favorables de FortiAuthenticator”:

Tabla 2 Características favorables de FortiAuthenticator.

| Característica | Detalles de la característica |
|---|---|
| RADIUS | Servidor de autenticación y autorización tipo RADIUS. |
| | Proxy de autenticación y cuentas de usuario. |
| | Sobre escritor de paquetes de RADIUS para utilizarlos en FSSO (Fortinet SSO). |
| Escalabilidad y doble factor de autenticación | Escalabilidad y manejo centralizado de usuarios (desde 100 a 1 millón de usuarios). |
| | Segundo factor con token físico, token móvil, mensaje de texto y correo electrónico. |
| Fortinet Single Sign On | Capacidades extendidas de SSO – Sobre SYSLOG y algunas API. |
| | Restricción de cantidad de dispositivos por usuario de FSSO |
| | Filtrado integrado de Firewall de siguiente generación marca Fortinet, por Usuario, grupo, dispositivo, dirección MAC e IP. |
| | FSSO con Kerberos (con retroceso NTLM) |
| | Proveedor de servicios SAML (Security Assertion Markup Language) (Con SSO en la nube) |
| | Proveedor de identidad SAML (Con SSO en la nube) |
| Directorio Activo | Auto sincronización con el directorio activo basado en reglas. |
| | Reinicio de la contraseña del directorio activo desde la plataforma. |
| WiFi/Hotspot | Autenticación social, basándose en los usuarios de Facebook, Twitter, Linkedin y Google. |
| Manejo de invitados y BYOD (Bring Your Own device) | Autoridad certificadora local |
| | Manejo de autenticación de clientes tipo Endpoint. |

Las anteriores razones dieron como resultado que el proyecto utilizara un FortiAuthenticator para realizar las pruebas de la autenticación tipo Enterprise, sobre todo por su integración con el directorio activo de Windows con el que ya cuenta la empresa.

## 4.3 MARCO CONTEXTUAL

La investigación será realizada dentro del marco del área de operaciones de la empresa Kappa10 Ltda., la cual cuenta con su sede principal en el país de Colombia, ciudad de Bogotá, localidad Chapinero. El área de la empresa sobre la cual se enfocará el análisis está compuesta por un ingeniero líder de soporte, un ingeniero líder de implementación, y tres ingenieros encargados de las labores de soporte nivel 1 y 2 e implementación.

El área tiene su principal centro de operaciones en la oficina 211 de la sede principal, y por su tipo de labores también es normal que haga uso del trabajo remoto como un medio alternativo de mantener al día sus actividades y responsabilidades, eso sí dentro de la misma ciudad de Bogotá en general. A continuación, en la tabla número 3, se listan algunos proyectos similares llevados a cabo en otras entidades.

Tabla 3 Proyectos similares.

| Nombre | Propósito del proyecto |
|---|---|
| Análisis de riesgos y recomendaciones de seguridad de la información del hospital E.S.E. San Bartolomé de Capitanejo, Santander[50] | Este trabajo buscó identificar los riesgos y generar las recomendaciones de acuerdo con los niveles de seguridad informática actual de los activos de infraestructura tecnológica del hospital E.S.E. San Bartolomé de Capitanejo, mediante un análisis de riesgo que abarcó las vulnerabilidades, riesgos, controles actuales, controles recomendados de mitigación de riesgo según ISO 27001, y un plan de sensibilización, difusión y capacitación en políticas de seguridad informática para los empleados de la entidad. Es interesante que los ingenieros Cordero y García realizaron el análisis con la ayuda de software especializado en la tarea, EAR/PILAR, una herramienta muy poderosa y efectiva para un SGSI. |
| Análisis de riesgos para una empresa de consultoría[51] | Este trabajo buscó comprender e identificar de forma global la manera de operación de la empresa sobre la cual se basó el trabajo, y enfocó su análisis a las áreas de operaciones y relaciones corporativas. Este documento se enfocó a la seguridad y salud en el trabajo. |
| Valoración y plan de tratamiento de riesgos de seguridad de la información para los procesos incluidos en el alcance del SGSI del cliente TGE de la empresa Assurance Controltech[52] | Este trabajo buscó identificar y evaluar los riesgos de seguridad de la información presentados en los procesos de Entrega personalizada y Call Center de la empresa TGE, cliente de Assurance Control Tech, y de acuerdo con esto el trabajo definió un PTR (Plan de tratamiento del Riesgo) a la medida de la empresa. Es importante destacar que en el documento presentado, los ingenieros a cargo del proyecto no solo se valieron de la norma ISO 31000, sino que también utilizaron las normas ISO 27001 y 27002 para dar un mayor respaldo a sus planteamientos, con los cuales se organizó y presentó el debido PTR. |
| Análisis de riesgos de seguridad y salud por procesos basado en la norma ISO 31000:2011 para el Grupo Alcomex[53] | Este trabajo buscó diseñar un análisis de riesgos de seguridad y salud por procesos para un operador logístico de servicios aduaneros, almacenamiento de mercancía y administración de inventarios, y logró identificar, analizar y evaluar los riesgos de esta empresa y generar las recomendaciones que se implementarían en esta. |

[50] CORDERO, José y GARCÍA, Yadimyr. Análisis de riesgos y recomendaciones de seguridad de la información del hospital E.S.E. San Bartolomé de Capitanejo. Trabajo de grado Especialista en seguridad informática. Málaga. Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas, Tecnologías e Ingenierías. 2016, 82p.

[51] PEREIRA MORALES, Ana y RODRIGUEZ LUNA, Yuly. Análisis de riesgos para una empresa de consultoría. Bogotá, 2016, 28p. Trabajo de grado (Especialista en gerencia de riesgos y seguros). Institución Universitaria Politécnico Grancolombiano. Facultad de Ingeniería.

[52] JARA PÉREZ, Diana. Valoración y plan de tratamiento de riesgos de seguridad de la información para los procesos incluidos en el alcance del SGSI del cliente TGE de la empresa Assurance Controltech. Trabajo de grado Ingeniería de Sistemas. Bogotá. Universidad Distrital Francisco José de Caldas. Facultad de Ingeniería. 2017. 58p.

[53] GUTIÉRREZ CONEO, Jesús y PINEDA ARIAS, Juan. Análisis de riesgos de seguridad y salud por procesos basado en la norma ISO 31000:2011 para el Grupo Alcomex. Trabajo de grado Ingeniería de Producción. Bogotá. Universidad Distrital Francisco José de Caldas. Facultad de Tecnología. 2016, 57p.

## 4.4 MARCO LEGAL

### 4.4.1 Normatividad a nivel nacional.

Cada vez que una empresa colombiana desea implementar un sistema de gestión de información o realizar un análisis de riesgos de sus activos informáticos, es necesario que consulte la legislación actual que rige en cuanto a este aspecto, por ejemplo, cosas como los derechos de autor, la propiedad industrial, la propiedad intelectual etc. A continuación, se verán las leyes colombianas que rigen sobre el proyecto aplicado “Análisis de riesgos de los sistemas de seguridad informática de la empresa kappa10 Ltda.”

LEY 1723 DE 2009 (enero 5 de 2009). Esta ley modificó el código penal colombiano, creando un nuevo bien jurídico tutelado, llamado “de la protección de la información y de los datos”[54] en cuanto a todo lo que tiene que ver con las TICs. En el artículo 269A menciona que nadie que no esté debidamente autorizado debe acceder a un sistema de información, sea que esté o no protegido con alguna medida de seguridad, lo que por sí mismo incluye que estos activos deben ser monitoreados y tener una trazabilidad que permita saber quién los accede y que hace en cada uno de ellos.

En los artículos 269B y 269D de esta ley, viene hablándose del sabotaje de un sistema informático o de telecomunicaciones y del daño informático, nuevamente, es importante resaltar que sin una trazabilidad de logs de usuarios sería prácticamente imposible probar uno de estos delitos, por lo que es imprescindible un sistema de autenticación y retención de registros confiable.

De acuerdo con la ley 1723 del 2009, la empresa Kappa 10 Ltda. faculta al ingeniero encargado del proyecto a hacer uso de sus datos no confidenciales, y solo algunos de sus datos confidenciales, como los nombres y configuraciones de hardware y

[54] REPUBLICA DE COLOMBIA. LEY 1273 DE 2009. [2009]. [en línea] [citado el 15 de octubre, 2018]. Disponible en internet: http://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

software de los servidores y equipos informáticos, su modo de operación, sus propósitos y manejos, más no al manejo de nombres de empleados, datos personales o empresariales, tablas de ingresos y egresos económicos, y en general todo lo que no tenga que ver con los activos informáticos de esta (Se anexa carta de autorización de gerencia).

LEY 719 DE 2001 (diciembre 24 de 2001). Esta ley habla sobre los derechos de autor, y como debe hacerse un reconocimiento a la propiedad de este, es por eso por lo que cualquier obra o trabajo citado en este proyecto llevará su debida nota a pie de página con las citaciones, de acuerdo con la norma NTC 5613, y también se referenciaran en la bibliografía del documento.

LEY ESTATUTARIA 1266 DE 2008 (diciembre de 2008). En esta ley se definen las disposiciones reglamentarias del hábeas data y el manejo de la información contenida en las bases de datos comerciales, crediticias, personales, financieras y de servicios[55].

[55] REPUBLICA DE COLOMBIA. LEY ESTATUTARIA 1266 DE 2008. [2008]. [en línea] [citado el 15 de octubre, 2018]. Disponible en internet: http://ticbogota.gov.co/node/137

# 5 DISENO METODOLÓGICO

El proyecto tiene un enfoque de investigación cuantitativo, ya que es un proyecto de ingeniería aplicada encaminado a tratar el tema de análisis de riesgos en entornos informáticos empresariales, así como la seguridad en sistemas de autenticación para el sector privado, lo que comprende la gestión de identidad dentro de los entornos empresariales. La línea de investigación eje del proyecto es la de “Infraestructura tecnológica y seguridad en redes”, que comprende la temática de “Redes industriales”.

## 5.1 TIPO DE INVESTIGACIÓN

La metodología por usar en este proyecto será la de investigación aplicada con un enfoque mixto, siguiendo los lineamientos y fases descritos en el siguiente aparte. Este tipo de investigación consiste en establecer el problema, previamente conocido por el investigador, y responder las preguntas específicas que se han hecho durante el periodo inicial.

La investigación aplicada se centra en el estudio y la resolución práctica de problemas, dando como resultado la puesta en marcha del conocimiento previamente adquirido por el estudiante, y generando las respuestas a los interrogantes planteados así como el conocimiento de las consecuencias de las acciones tomadas dentro de cierto campo especifico.

De acuerdo con la metodología MAGERIT y el modo de aplicación escogido para poder llegar a un buen término del proyecto, las fases de este van desde el surgimiento de la idea hasta la evaluación de sus resultados. Las seis fases que identifican el ciclo de vida del proyecto aplicado son:

1. *Levantamiento de información:*

En esta fase se recogen datos e información importante para el proyecto por medio de consultas de bibliografía, encuestas, entrevistas, visitas de campo, e indicadores, lo que principalmente se traduce en la realización completa de un estudio observacional[56]. Con este aparte se da cumplimiento al objetivo específico número uno, a saber, "realizar el inventario de activos de infraestructura tecnológica de la empresa Kappa10"

2. *Análisis de situación actual:*

Para este momento se tiene la información de la fase anterior, por lo que debe organizarse de manera coherente, para definir las actividades y recursos necesarios para lograr los objetivos concretos del proyecto[57]. Estas dos primeras fases son fundamentales, ya que ponen las bases para el éxito de las siguientes etapas del proyecto. Con este aparte se complementa el cumplimiento del objetivo específico número uno.

3. *Desarrollo del análisis de riesgos:*

En esta fase, con los datos claros y organizados, se elabora el análisis de riesgos correspondientes a la empresa Kappa10 Ltda., y se socializa con la empresa por medio de entrevistas y exposiciones donde se explicarán las causas y efectos del proyecto. Con este aparte se da cumplimiento al objetivo específico número dos, a saber, "Realizar el análisis de riesgos actuales de la empresa Kappa10 Ltda."

---

[56] JAUREGUI, Macarena. Los datos estadísticos: tipos y técnicas de obtención [2016]. [en línea] [citado el 16 de mayo, 2018]. Disponible en internet: https://aprendiendoadministracion.com/los-datos-estadisticos-tipos-y-tecnicas-de-obtencion/

[57] ALOMÍA ARCE, Hernán; ESCALLÓN SANTAMARÍA, Víctor y ORTEGÓN MOSQUERA, Katherine. Metodología para realización de proyectos de grado departamento de ingeniería industrial. [2007]. [en línea] [citado el 16 de mayo, 2018]. Disponible en internet: ftp://ftp.icesi.edu.co/leonardo/PGI/Guia%20Estudiantes.pdf

4. *Aplicación del análisis de riesgos (Al riesgo particular de gestión de identidad):*

Inmediatamente después de la fase anterior, con la documentación del análisis de riesgo completa como insumo, se comienza esta fase, que es en la cual se atacará uno de los riesgos actuales detectados en la infraestructura informática de la compañía, a saber, la falta de gestión de identidad en el área operativa. En esta fase se obtendrán los materiales necesarios para poner en marcha el piloto de la solución propuesta. Los materiales pendientes por obtener son:

- Implementación en general de la máquina virtual de FortiAuthenticator con licencia de prueba (El servidor físico donde será montada y operará esta máquina virtual ya está disponible dentro de los activos de la empresa).

En esta sección se da cumplimiento al objetivo específico número tres, a saber, "Determinar los controles para cada riesgo detectado dentro del análisis."

5. *Ejecución y seguimiento:*

En esta etapa es donde se realizará la prueba piloto de la solución propuesta, y se divide en las siguientes actividades:

- Montaje de la máquina virtual de FortiAuthenticator.
- Prueba piloto con equipos de laboratorio de la marca Fortinet propios de Kappa10.

En esta sección se da cumplimiento al objetivo específico número cinco, a saber, "Realizar un laboratorio controlado que sirva de paso inicial para la mitigación de los riesgos de gestión de identidad de la empresa."

6. *Socialización y evaluación de resultados:*

En esta fase se realizará una socialización a la empresa, donde se darán a conocer los resultados, los hallazgos y recomendaciones que se obtuvieron del

análisis de riesgos a lo largo del proyecto. Adicionalmente se mostrarán los resultados de la prueba piloto como posible solución de mitigación del riesgo de gestión de identidad existente. Con base en estos resultados se realizará una evaluación del proyecto desde el punto de vista de la empresa que recibe. Posteriormente se socializará el proyecto en general con el jurado de la UNAD.

Finalmente, en esta parte se da cumplimiento al objetivo específico número cuatro, a saber, “Generar un documento con las recomendaciones de seguridad informática surgidas a raíz del análisis de riesgos realizado”.

## 5.2 FUENTES Y TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN

Con este método de investigación la recopilación de datos se apoyará mayormente mediante entrevistas, encuestas, visitas de campo, revisión de bases de datos propias y externas, e indicadores tomados de la infraestructura actual de la empresa de estudio.

### 5.2.1 Fuentes primarias

Las fuentes primarias son las que involucran contacto directo con los sujetos, objetos y procesos directamente relacionados con el proyecto de investigación, por lo que en este entorno serán las definidas a continuación:

- Entrevistas: En estas entrevistas el investigador tratará de ahondar en el problema mediante la opinión de los actores directamente implicados en los procesos, los actores externos, y el área de cumplimiento de la empresa, todo enfocado hacia el cumplimiento de normas para obtener la certificación ISO 27001.
- Encuestas: Realizadas mayormente por medios electrónicos dentro de la misma empresa, con el fin de evitar gasto innecesario de recursos físicos de

papelería. Estas encuestas podrán contener preguntas abiertas (En las cuales la respuesta será de acuerdo con la persona que la responda), o preguntas cerradas (en las que se delimitarán las opciones de respuesta).

- Observación: Esta recolección se realizará mediante visitas de campo que permitan al investigador identificar realmente los riesgos informáticos de la compañía en cuestión.
- Indicadores de la infraestructura actual: Estos indicadores se tomarán de los registros de máquinas reales administradas por la empresa, así como de la herramienta de software en donde se registran los casos solicitados por clientes.

### 5.2.2 Fuentes secundarias

Las fuentes secundarias son las que hacen referencia a documentos, fotos, grabaciones de audio y video, e información consultada en Internet, que no están directamente relacionados con el proyecto de investigación, por lo que en este entorno serán las definidas a continuación:

- Análisis de documentación: Mayormente desde Internet, tomando como base los casos de éxito en otras empresas a manera de consulta, e investigación de la documentación técnica del fabricante.

## 5.3 DELIMITACIÓN Y ALCANCE

Este proyecto comprende la realización de un análisis de riesgos del cual se obtendrán las respectivas recomendaciones de mitigación de riesgos de la infraestructura tecnológica de la empresa colombiana Kappa10 Ltda. Adicionalmente, comprende la implementación de la prueba piloto de un sistema de autenticación tipo Enterprise con equipos de laboratorio y licencias de prueba del

fabricante Fortinet dentro de las instalaciones de la empresa. A continuación la delimitación del proyecto:

- Delimitación temporal: Hace referencia al periodo de tiempo entre el cual se ejecutará el proyecto. El periodo de aplicación del proyecto está comprendido entre el 23 de agosto y el 12 de diciembre del 2018, fechas en las que transcurre el segundo periodo de 16 semanas del calendario educativo de la UNAD.
- Delimitación geográfica: Hace referencia al lugar donde se ejecutará el proyecto, en este caso es la empresa Kappa10 Ltda. ubicada en la ciudad de Bogotá, Colombia.

## 5.4 POBLACIÓN Y MUESTRA

La población sobre la cual se realizará el proyecto son los activos informáticos de la empresa Kappa 10 Ltda., especialmente los activos que pertenecen al área de operaciones. Al tratarse de un número pequeño y limitado de activos, no se tendrá una población muestra, sino que todos los activos harán parte del proyecto aplicado, llegando la población y la muestra a ser iguales en cantidad. Se delimitó el proyecto de esta forma, es decir, dejando de lado activos generales de la empresa como computadoras de usuarios, con el fin de centrar la atención a los activos que atañen al Core del negocio, como servidores y elementos esenciales de red, y cuya afectación supondría perdidas para la empresa. De esta manera se focaliza el análisis desde un punto de vista más acotado para ser presentado a la gerencia de Kappa10 Ltda.

# 6 DESARROLLO DE LA PROPUESTA

## 6.1 INVENTARIO INFRAESTRUCTURA TECNOLOGICA DE KAPPA10

Por medio de una entrevista realizada el mes de septiembre del 2018 con el área de cumplimiento de la empresa Kappa10 Ltda. se hizo un levantamiento de información de los activos informáticos de esta, y se adelantó una matriz de riesgos en formato Excel para comenzar a realizar el análisis de riesgos informáticos de cada uno de estos.

Una vez diligenciada esta matriz, se realizarán las recomendaciones a la empresa con el fin de mitigar los riesgos encontrados y que así puedan adquirir la certificación ISO 27001. Adicionalmente, se realizarán visitas de investigación y recolección de datos de los activos de la empresa durante la primera semana de octubre, con el fin de corroborar lo recibido el día de la entrevista. De forma paralela se cumplirá el objetivo específico número 4, que hace referencia al laboratorio de autenticación tipo Enterprise.

Lo diligenciado en la tabla 4 “Activos de infraestructura tecnológica de Kappa10”, corresponde al inventario tecnológico de la empresa Kappa 10 Ltda., y contiene los activos de información valiosos de la empresa, en torno a los cuales giran los servicios importantes que presta la compañía a sus clientes y aliados:

Tabla 4 Activos de infraestructura tecnológica de Kappa10.

| Proceso | Activo | Tipo de activo | Propietario | Ubicación | Clasificación de riesgo | Servicio |
|---|---|---|---|---|---|---|
| Operación | FortiWifi 60D-POE<br>Marca: Fortinet<br>Ser.FW60DP4615000576 | Tangible | Área de operaciones | Kappa 10 Oficina 503. Rack 1. | Crítico | Filtrado UTM, navegación oficina 503. |
| Operación | FortiGate 60D<br>Marca: Fortinet<br>Ser.FGT60D4Q16035223 | Tangible | Área de operaciones | Kappa 10 Oficina 211. Rack 1. | Importante | Filtrado UTM, navegación oficina 211. |
| TI | Cámara_OF503<br>Marca: Dahua<br>Ser. 1E02139PAL00034 | Tangible | Área de TI | Kappa 10 Oficina 503. | Bajo | Seguridad física oficina 503. |

Tabla 4. (Continuación)

| | | | | | | |
|---|---|---|---|---|---|---|
| TI | Cámara_OF211<br>Marca: IDTX<br>Ser. RCIP02720-201703 | Tangible | Área de TI | Kappa 10 Oficina 211. | Bajo | Seguridad física oficina 211. |
| TI | Chromecast<br>Marca: Google<br>Ser. 5807103XJQKN | Tangible | Área de TI | Kappa 10 Oficina 211. | Bajo | Servicios de proyección en reuniones. |
| Operación | FortiAP 221B<br>Marca: Fortinet<br>Ser. FP221B3X13012005 | Tangible | Área de operaciones | Kappa 10 Oficina 211. | Importante | Servicio de red inalámbrica oficina 211. |
| Operación | FortiAP PU423E<br>Marca: Fortinet<br>Ser. PU423E3X16003228 | Tangible | Área de operaciones | Kappa 10 Oficina 503. | Importante | Servicio de red inalámbrica oficina 503. |
| Operación | FortiWifi 60C<br>Marca: Fortinet<br>Ser. FWF60C3G12006002 | Tangible | Área de operaciones | Kappa 10 Oficina 211. Rack 1. | Despreciable | Servicio de pruebas de laboratorio de operaciones. |
| TI | Telefóno IP Recepción<br>Marca: GranStream<br>Ser. GP2160-0313576741 | Tangible | Área de TI | Kappa 10 Oficina 503. | Importante | Recepción y salida de llamadas. |
| Operación | Switch Catalyst 2960<br>Marca: Cisco<br>Ser. WSC2950G48EI | Tangible | Área de operaciones | Kappa 10 Oficina 211. Rack 1. | Importante | Interconexión de servidores y equipos Rack 1 oficina 503. |
| TI | PBX UCM6104<br>Marca: Grandstream<br>Ser. 21AWLS8G409205FA | Tangible | Área de TI | Kappa 10 Oficina 503. Rack 1. | Importante | Control de llamadas. |
| Operación | Modem ISP (ETB)<br>Marca: ZTE<br>Ser. ZTEGC04F2997 | Tangible | Área de operaciones | Kappa 10 Oficina 503. Rack 1. | Crítico | Canal de Internet oficina 503. |
| Operación | Modem ISP (ETB)<br>Marca: ZTE<br>Ser. ZTEGC0B75BD7 | Tangible | Área de operaciones | Kappa 10 Oficina 211. Rack 1. | Importante | Canal de Internet oficina 211. |
| TI | Impresora M127NF<br>Marca: HP<br>Ser. CNBH7P47D | Tangible | Área de TI | Kappa 10 Oficina 503. | Bajo | Impresión de documentos empresariales. |

Tabla 4. (Continuación)

| | | | | | | |
|---|---|---|---|---|---|---|
| TI | UPS PRO1500<br>Marca: APC<br>Ser. 4B1520P45549 | Tangible | Área de TI | Kappa 10 Oficina 503. Rack 1. | Importante | Supresor de picos de voltaje y continuidad de alimentación de servidores y equipos de comunicación principales. |
| Operación | FortiAutenticator VM (Apagado) | Intangible | Área de operaciones | Kappa 10 Oficina 503. Servidor Principal | Critico | Máquina virtual. Apagada por el momento. |
| TI | FE-ITOP (VM)<br>MV de pruebas (Apagado) | Intangible | Área de TI | Kappa 10 Oficina 503. Servidor Principal | Despreciable | Máquina virtual. Apagada por el momento. |
| TI | Servidor principal<br>Marca: HP<br>PROLIANT ML 30 G9<br>Ser. MX26060006K | Tangible | Área de TI | Kappa 10 Oficina 503. Rack 1. | Critico | Servidor de aplicaciones principales. |
| Operación | Servidor Laboratorio<br>Marca: Lenovo<br>M72e Desktop (ThinkCentre)<br>Ser. MJTZLWY | Tangible | Área de operaciones | Kappa 10 Oficina 211. Rack 1. | Apreciable | Servidor de aplicaciones de prueba. |
| TI | Servidor Contabilidad WO<br>Marca: HP<br>PROLIANT MICROSERVER<br>Ser. MX25210009 | Tangible | Área de TI | Kappa 10 Oficina 503. Rack 1. | Critico | Servidor de aplicación de contabilidad. |
| TI | UPS GALLEON 3K X9<br>Marca: Energex<br>Ser. 83311412100086 | Tangible | Área de TI | Kappa 10 Oficina 211. Rack 1. | Bajo | Supresor de picos de voltaje y continuidad de alimentación de servidores y equipos de comunicación principales. |

Tabla 4. (Continuación)

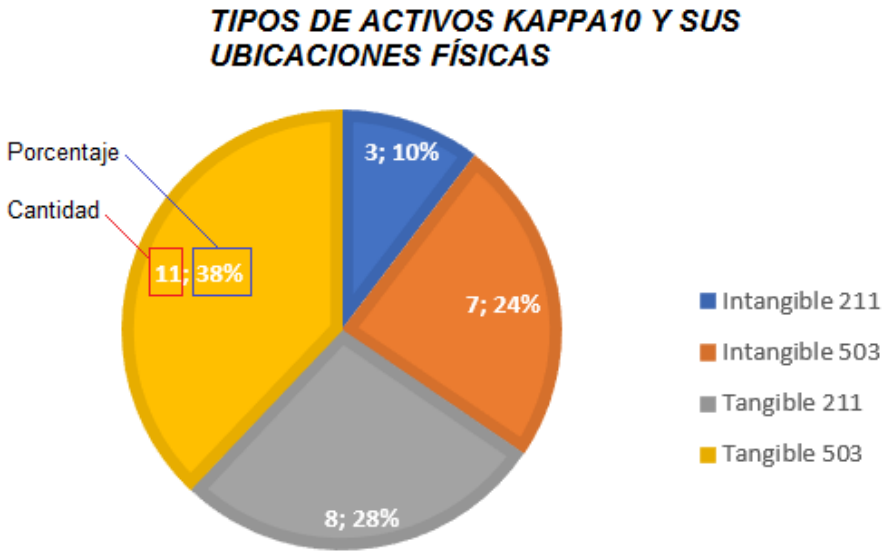
| | | | | | | |
|---|---|---|---|---|---|---|
| Compras / Financiero / Operación / TI | Aplicación ITOP | Intangible | Área de TI | Kappa 10 Oficina 503. Servidor Principal | Crítico | Base de datos comercial y de ingeniería de Kappa 10 Ltda. |
| Compras / Financiera | Aplicación SIIGO | Intangible | Área de TI | Kappa 10 Oficina 503. Servidor Contabilidad WO | Critico | Aplicación de contabilidad de Kappa 10 Ltda. |
| Operación | FortiManager VM Marca: Fortinet Ser. FMG-VMTM18000131 | Intangible | Área de operaciones | Kappa 10 Oficina 211. Servidor Laboratorio | Bajo | Máquina Virtual. Para servicios de revisión previsiva en clientes. |
| Operación | PRTG Network Monitor Marca: Paessler AG | Intangible | Área de operaciones | Kappa 10 Oficina 211. Servidor Laboratorio | Apreciable | Aplicación de prueba de registro y alerta de problemas en equipos de redes. |
| TI | Domain Controller Marca: Windows | Intangible | Área de TI | Kappa 10 Oficina 503. Servidor Principal | Critico | Servicio de control de usuarios y dispositivos. |
| Operación | Servicio de Internet 1 ISP: ETB | Intangible | Área de operaciones | Kappa 10 Oficina 503. Rack 1. | Critico | Servicio de Internet de la oficina principal. |
| Operación | Servicio de Internet 2 ISP: ETB | Intangible | Área de operaciones | Kappa 10 Oficina 211. Rack 1. | Importante | Servicio de Internet de la oficina secundaria. |
| TI | Servicio de telefonía IP | Intangible | Área de TI | Kappa 10 Oficina 503. | Bajo | Servicio de telefonía IP. |

Fuente: Juan Carlos Briceño

La tabla 4 se recolectó con base en la información documentada en el software iTop, la información visualizada en las visitas y lo obtenido en las entrevistas con los ingenieros encargados de cada recurso, y se obtuvo con el propósito de hacer el análisis más acertado con respecto a la infraestructura tecnológica de la empresa.

La figura 3 muestra el tipo y porcentaje de activos de infraestructura informática de la empresa, obtenidos de las revisiones realizadas durante el análisis y expuestas en la tabla 4 “Activos de infraestructura tecnológica de Kappa10” que se encuentra detallada a partir de la página 54 de este documento. La mayoría de estos activos son tangibles (66%) debido a que se refiere al hardware donde corren las aplicaciones, o a equipos de red necesarios para el día a día de la operación. El restante 34% se refiere a activos intangibles, como aplicaciones de inventarios, bases de datos y maquinas virtuales.

Figura 3. Gráfica de la tabla 4.




Fuente: Juan Carlos Briceño.

La recolección de datos de los activos se realizó en dos fases. La primera fase incluyó la entrevista al profesional de TI y la revisión de la base de datos de activos tecnológicos de la empresa por medio del software iTop. Por medio de realizar una

exportación de la base de activos a un formato de Excel se consiguió gran parte de la información.

En la segunda fase, se realizaron visitas de recolección de información visual a las dos oficinas de la empresa, y se tomaron registros fílmicos que se muestran en el anexo A de este documento para dar un mayor entendimiento de la situación (Ver Anexo A).

Durante la inspección visual realizada se pudieron notar varias cosas que serán de mucha ayuda durante el análisis, por ejemplo, en la tabla 5 “Hallazgos visuales Kappa 10 Ltda”, se describen varios de los hallazgos importantes, y en el Anexo A se encuentran los registros fílmicos que corroboran esta información:

Tabla 5 Hallazgos visuales Kappa 10 Ltda.

| Lugar | Hallazgo visual | Observaciones |
|---|---|---|
| Oficinas 211 y 503 | Las dos oficinas cuentan con puertas que poseen doble cerradura, lo que permite tener un mayor nivel de seguridad física. | Hallazgo de seguridad física. |
| Oficinas 211 y 503 | Los racks no se encuentran en un centro de cómputo, sino en las oficinas. | La razón es que la empresa tiene en alquiler únicamente 2 oficinas del edificio en el que se encuentra, y no centros de cómputo. |
| Oficina 503 | Rack con llave, y asegurado con tornillos especiales tipo Bristol. Además se encuentra anclado al piso y con polo a tierra definido. | |
| Oficina 211 | Rack con llave, y asegurado con tornillos especiales tipo Bristol. Además se encuentra anclado al piso y con polo a tierra definido. | |
| Oficinas 211 y 503 | Las cámaras de vigilancia y los Access points, están a la altura del techo, que en ambos casos supera los 3 metros, por lo que se considera adecuada su seguridad ya que no son fácilmente manipulables. | |
| Oficina 503 | No hay red cableada, solamente red Wifi. | La red Wifi tiene si SSID escondido y con clave, lo que se considera seguro. |
| Oficina 503 | Se tiene un registro de ingreso de personal externo como medida adicional a las cámaras. | La bitácora se encuentra en la recepción de la oficina. |
| Oficina 211 | Solo tiene dos puntos de red cableados, correctamente marcados en el patch panel y en el punto como tal, para evitar confusiones. | Marquillado correcto. |
| Oficina 211 | Solo ingresa personal de la empresa, por lo que no se tienen registros de ingreso físicos. | La cámara suple la necesidad de un registro físico, ya que solo ingresa personal autorizado previamente. |

## 6.2 ANALISIS DE RIESGOS DE KAPPA10

El alcance del análisis de riesgos comprende el diseño de un plan de tratamiento de riesgos para los 69 ítems de nivel inaceptable, que son los considerados más urgentes de corrección y mitigación dentro de la empresa. Este análisis se realizó mediante la matriz de análisis de riesgos diligenciada en conjunto con las áreas de cumplimiento y operaciones de la empresa (Por favor ver el Anexo C). Dicha matriz se anexa al proyecto como parte de la documentación de este.

Es muy importante aclarar varios puntos previos al análisis realizado:

- El alcance del análisis aplica para los activos de infraestructura tecnológica de la Empresa.
- El alcance del plan de tratamiento del riesgo (PTR) comprende los riesgos de clasificación “Inaceptable”, sobre los cuales se basarán las recomendaciones a Kappa 10 Ltda.
- En principio se dará prioridad a mitigar los riesgos sobre los activos y procesos más importantes.

### 6.2.1 Valoración de activos

Una vez aclarado este alcance, es necesario entender la forma en la cual se clasificaron los activos de infraestructura tecnológica de acuerdo con la metodología propuesta. La clasificación es el insumo que permite identificar cuales activos son críticos, cuales importantes, cuales medios y cuales bajos o despreciables durante el análisis de riesgos.

La clasificación se realizó con base en las entrevistas, documentación y reuniones sostenidas al interior de la empresa, las cuales arrojaron valores que se estandarizaron y normalizaron mediante la matriz de análisis de riesgos adjunta a este documento. En la tabla 6 “Parámetros de valoración de activos” se muestran

las diferentes variables que sirvieron como base para realizar la valoración de cada activo:

Tabla 6 Parámetros de valoración de activos.

| Variable | Definición | Observaciones | Ejemplo |
|---|---|---|---|
| Activo | Nombre del activo de infraestructura tecnológica. | | [HW_FORTIWIFI_60D-POE] |
| Tipo de activo | Clasificación del activo de acuerdo con su forma física o lógica. | Pueden ser de los siguientes tipos:<br>(D) DATOS<br>(K) CLAVES CRIPTOGRAFICAS<br>(S) SERVICIOS<br>(SW) SOFTWARE<br>(HW) EQUIPAMENTO INFORMÁTICO<br>(COM) REDES DE COMUNICACIONES<br>(Media) SOPORTE DE INFORMACIÓN<br>(AUX) EQUIPAMENTO AUXILIAR<br>(L) INSTALACIONES<br>(P) PERSONAL | [HW] EQUIPAMENTO INFORMÁTICO |
| Dimensión | Son cinco dimensiones, sobre las cuales debe darse un valor cualitativo, que puede ser “Muy Bajo”, “Bajo”, “Medio”, “Alto” y “Muy alto”. De acuerdo con el valor definido se marcará un valor cuantitativo en otra tabla para arrojar resultados. | Las cinco dimensiones son:<br>1. Dimensión Autenticidad<br>2. Dimensión Trazabilidad<br>3. Dimensión Confidencialidad<br>4. Dimensión Integridad<br>5. Dimensión Disponibilidad | 1. Dimensión Autenticidad: **Alto**<br>2. Dimensión Trazabilidad: **Alto**<br>3. Dimensión Confidencialidad: **Muy alto**<br>4. Dimensión Integridad: **Alto**<br>5. Dimensión Disponibilidad: **Muy alto** |
| Atributos | Representan cosas como si el activo contiene información confidencial de terceros, si debe ser de uso restringido, si puede verse comprometido en fraudes, si es muy crítico para las operaciones de la empresa, o si es muy crítico para dar servicio a terceros. | Son siete preguntas, que dependiendo de si son o no afirmativas, se les asigna un valor cuantitativo que más adelante servirá para obtener el valor numérico del activo para la empresa. | Activo de información que puede ser alterado o comprometido para fraudes o corrupción: **Si** |
| Ubicación | Permite saber dónde se encuentra el activo, si está en forma física o electrónica. | | Ubicación: **Física.** |

Una vez se completa la información en la tabla, la matriz cuantifica en valor y la importancia de cada activo mediante la asignación de valores a cada una de las dimensiones y atributos examinados en la valoración cualitativa. Con el promedio de estos valores redondeado, se obtiene finalmente el valor numérico de cada activo, lo cual facilita enormemente el proceso de clasificación y evaluación de riesgos. La tabla 7 “Valoración de activos” describe los parámetros de la valoración realizada:

Tabla 7 Valoración de activos.

| VALORACIÓN DEL RIESGO | | | |
|---|---|---|---|
| | **Nomenclatura** | **Categoría** | **Valoración** |
| **Valoración del riesgo** | MA | Crítico | 21 a 25 |
| | A | Importante | 16 a 20 |
| | M | Apreciable | 10 a 15 |
| | B | Bajo | 5 a 9 |
| | MB | Despreciable | 1 a 4 |

De acuerdo con la información recolectada, y al método de valoración de activos estudiado, los activos de infraestructura tecnológica de Kappa10 Ltda. se ven distribuidos en las cinco categorías de acuerdo con la tabla 8 “Valoración de activos Kappa10” (Para ver la tabla completa por favor remitirse al archivo adjunto “Matriz de Análisis de Riesgos Kappa10.xlsx” pestaña “Valoración Cuantitativa”):

Tabla 8 Valoración de activos Kappa10.

| Nombre | Riesgo | Valor |
|---|---|---|
| [HW_FORTIWIFI_60D-POE] | CRITICO | 22 |
| [HW_FORTIGATE_60D] | IMPORTANTE | 19 |
| [D_DOMAIN_CONTROLLER] | CRITICO | 21 |
| [AUX_CAMARA-OF503] | BAJO | 8 |
| [AUX_CAMARA-OF211] | BAJO | 8 |
| [HW_CHROMECAST] | DESPRECIABLE | 4 |
| [HW_FORTIAP_211B] | IMPORTANTE | 20 |
| [HW_FORTIAP_PU423E] | IMPORTANTE | 19 |
| [HW_FORTIWIFI_60C] | DESPRECIABLE | 4 |
| [HW_TELEFONO_IP_RECEP.] | IMPORTANTE | 19 |
| [HW_SWITCH_CATALYST_2960] | IMPORTANTE | 19 |

Tabla 8. (Continuación)

| Nombre | Riesgo | Valor |
|---|---|---|
| [HW_PBX_UCM6104] | IMPORTANTE | 19 |
| [HW_MODEM_ISP_OF503] | CRITICO | 22 |
| [HW_MODEM_ISP_OF211] | IMPORTANTE | 20 |
| [HW_IMPRESORA_M127NF] | BAJO | 8 |
| [AUX_UPS_PRO1500] | IMPORTANTE | 16 |
| [SW_VM_FORTIAUTHENTICATOR] | CRITICO | 22 |
| [SW_FE_ITOP] | DESPRECIABLE | 4 |
| [HW_SRV_PRINCIPAL] | CRITICO | 22 |
| [HW_SRV_LABORATORIO] | APRECIABLE | 15 |
| [HW_SRV_CONTABILIDAD] | CRITICO | 23 |
| [AUX_UPS_GALLEON_3KX9] | BAJO | 8 |
| [SW_ITOP] | CRITICO | 24 |
| [SW_SIIGO] | CRITICO | 22 |
| [SW_VM_FORTIMANAGER] | BAJO | 6 |
| [SW_PRTG] | APRECIABLE | 15 |
| [SERVICE_INTERNET_OF503] | CRITICO | 21 |
| [SERVICE_INTERNET_OF211] | IMPORTANTE | 17 |
| [SERVICE_TELEPHONE] | BAJO | 7 |

### 6.2.2 Identificación de amenazas

El proceso de identificación de amenazas se realizó con base en la documentación propuesta en el libro 2 de la metodología MAGERIT versión 3[58]. De acuerdo con MAGERIT las amenazas pueden ser categorizadas en cuatro diferentes grupos, dentro de los cuales se encuentran tipificadas específicamente con su debida nomenclatura, tipos de activos que puede afectar, dimensiones, y descripción, como se observa en la tabla 9 “Clasificación de amenazas”:

Tabla 9 Clasificación de amenazas[59].

| TIPO AMENAZA | AMENAZA |
|---|---|
| [N] Desastres naturales | [N1] Fuego |
| [N] Desastres naturales | [N2] Daños por agua |
| [N] Desastres naturales | [N*] Desastres naturales |
| [I] De origen industrial | [I1] Fuego |

[58] GOBIERNO DE ESPAÑA. MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro 2. [2012]. Madrid. [en línea]. p. 25. Disponible en internet: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.W9NdSTFRepo

[59] UNAD. Matriz de Análisis de Riesgos FERZAMHER. [2018]. [en línea] [citado el 16 de mayo, 2018]. Disponible en internet: http://campus07.unad.edu.co/ecbti34/pluginfile.php/1396/mod_forum/attachment/43184/Matriz%20de%20Analisis%20de%20Riesgos%20FERZAMHER%20d.xlsx

Tabla 9. (Continuación)

| | |
|---|---|
| [I] De origen industrial | [I2] Daños por agua |
| [I] De origen industrial | [I*] Desastres industriales |
| [I] De origen industrial | [I3] Contaminación mecánica |
| [I] De origen industrial | [I4] Contaminación electromagnética |
| [I] De origen industrial | [I5] Avería de origen físico o lógico |
| [I] De origen industrial | [I6] Corte del suministro eléctrico |
| [I] De origen industrial | [I7] Condiciones inadecuadas de temperatura o humedad |
| [I] De origen industrial | [I8] Fallo de servicios de comunicaciones |
| [I] De origen industrial | [I9] Interrupción de otros servicios y suministros esenciales |
| [I] De origen industrial | [I10] Degradación de los soportes de almacenamiento de la información |
| [I] De origen industrial | [I11] Emanaciones electromagnéticas |
| [E] Errores y fallos no intencionados | [E1] Errores de los usuarios |
| [E] Errores y fallos no intencionados | [E2] Errores del administrador |
| [E] Errores y fallos no intencionados | [E3] Errores de monitorización (log) |
| [E] Errores y fallos no intencionados | [E4] Errores de configuración |
| [E] Errores y fallos no intencionados | [E7] Deficiencias en la organización |
| [E] Errores y fallos no intencionados | [E8] Difusión de software dañino |
| [E] Errores y fallos no intencionados | [E9] Errores de [re-]encaminamiento |
| [E] Errores y fallos no intencionados | [E10] Errores de secuencia |
| [E] Errores y fallos no intencionados | [E14] Escapes de información |
| [E] Errores y fallos no intencionados | [E15] Alteración accidental de la información |
| [E] Errores y fallos no intencionados | [E18] Destrucción de información |
| [E] Errores y fallos no intencionados | [E19] Fugas de información |
| [E] Errores y fallos no intencionados | [E20] Vulnerabilidades de los programas (software) |
| [E] Errores y fallos no intencionados | [E21] Errores de mantenimiento / actualización de programas (software) |
| [E] Errores y fallos no intencionados | [E23] Errores de mantenimiento / actualización de equipos (hardware) |
| [E] Errores y fallos no intencionados | [E24] Caída del sistema por agotamiento de recursos |
| [E] Errores y fallos no intencionados | [E25] Pérdida de equipos |
| [E] Errores y fallos no intencionados | [E28] Indisponibilidad del personal |
| [A] Ataques intencionados | [A3] Manipulación de los registros de actividad (log) |
| [A] Ataques intencionados | [A4] Manipulación de la configuración |
| [A] Ataques intencionados | [A5] Suplantación de la identidad del usuario |
| [A] Ataques intencionados | [A6] Abuso de privilegios de acceso |
| [A] Ataques intencionados | [A7] Uso no previsto |
| [A] Ataques intencionados | [A8] Difusión de software dañino |
| [A] Ataques intencionados | [A9] [Re-]encaminamiento de mensajes |
| [A] Ataques intencionados | [A10] Alteración de secuencia |
| [A] Ataques intencionados | [A11] Acceso no autorizado |
| [A] Ataques intencionados | [A12] Análisis de tráfico |
| [A] Ataques intencionados | [A13] Repudio |
| [A] Ataques intencionados | [A14] Interceptación de información (escucha) |
| [A] Ataques intencionados | [A15] Modificación deliberada de la información |
| [A] Ataques intencionados | [A18] Destrucción de información |
| [A] Ataques intencionados | [A19] Divulgación de información |
| [A] Ataques intencionados | [A22] Manipulación de programas |
| [A] Ataques intencionados | [A23] Manipulación de los equipos |
| [A] Ataques intencionados | [A24] Denegación de servicio |
| [A] Ataques intencionados | [A25] Robo |
| [A] Ataques intencionados | [A26] Ataque destructivo |
| [A] Ataques intencionados | [A27] Ocupación enemiga |
| [A] Ataques intencionados | [A28] Indisponibilidad del personal |
| [A] Ataques intencionados | [A29] Extorsión |
| [A] Ataques intencionados | [A30] Ingeniería social (picaresca) |

Con lo anterior en mente, se realizó la identificación de amenazas de cada uno de los activos de infraestructura tecnológica de Kappa10, siguiendo los lineamientos presentados en los libros 1 y 2 de MAGERIT[60]. De los 29 activos de infraestructura tecnológica presentes en la empresa, se encontraron un total de 291 amenazas, dando un promedio de 10 amenazas por cada activo. A continuación en la tabla 10 "Cantidad de amenazas por activo" se encuentra una estadística del número de amenazas identificadas por cada activo:

Tabla 10 Cantidad de amenazas por activo.

| Activo | Cantidad de amenazas |
|---|---|
| [AUX_CAMARA-OF211] | 10 |
| [AUX_CAMARA-OF503] | 10 |
| [AUX_UPS_GALLEON_3KX9] | 6 |
| [AUX_UPS_PRO1500] | 6 |
| [D_DOMAIN_CONTROLLER] | 10 |
| [HW_CHROMECAST] | 8 |
| [HW_FORTIAP_211B] | 10 |
| [HW_FORTIAP_PU423E] | 10 |
| [HW_FORTIGATE_60D] | 10 |
| [HW_FORTIWIFI_60C] | 10 |
| [HW_FORTIWIFI_60D-POE] | 10 |
| [HW_IMPRESORA_M127NF] | 10 |
| [HW_MODEM_ISP_OF211] | 10 |
| [HW_MODEM_ISP_OF503] | 10 |
| [HW_PBX_UCM6104] | 10 |
| [HW_SRV_CONTABILIDAD] | 11 |
| [HW_SRV_LABORATORIO] | 11 |
| [HW_SRV_PRINCIPAL] | 11 |
| [HW_SWITCH_CATALYST_2960] | 11 |
| [HW_TELEFONO_IP_RECEP.] | 11 |
| [SERVICE_INTERNET_OF211] | 8 |
| [SERVICE_INTERNET_OF503] | 8 |
| [SERVICE_TELEPHONE] | 8 |
| [SW_FE_ITOP] | 12 |
| [SW_ITOP] | 12 |
| [SW_PRTG] | 10 |
| [SW_SIIGO] | 12 |
| [SW_VM_FORTIAUTHENTICATOR] | 16 |
| [SW_VM_FORTIMANAGER] | 10 |
| **TOTAL** | **291** |

En resumen, los datos más destacables de la fase de identificación de amenazas son cosas como, que en total se presentaron **36 tipos diferentes de amenazas**,

[60] GOBIERNO DE ESPAÑA. MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro 1. [2012]. Madrid. [en línea]. p. 27. Disponible en internet: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.W9NdSTFRepo

que la amenaza más concurrente en los activos de infraestructura tecnológica de Kappa10 es la “avería de origen físico o lógico”, con 25 apariciones en el análisis, seguida de el “corte de suministro eléctrico” con 24 apariciones y en tercer lugar con 23 eventos los “errores del administrador”, mostrando así el panorama expuesto en la tabla 11 “Cantidad de amenazas por ocurrencia”:

Tabla 11 Cantidad de amenazas por ocurrencia.

| Tipo de amenaza MAGERIT | Cantidad de ocurrencias |
|---|---|
| [I5] Avería de origen físico o lógico | 25 |
| [I6] Corte del suministro eléctrico | 24 |
| [E2] Errores del administrador | 23 |
| [I8] Fallo de servicios de comunicaciones | 18 |
| [I1] Fuego | 16 |
| [A6] Abuso de privilegios de acceso | 14 |
| [E4] Errores de configuración | 14 |
| [E18] Destrucción de información | 13 |
| [E1] Errores de los usuarios | 10 |
| [E15] Alteración accidental de la información | 10 |
| [E23] Errores de mantenimiento / actualización de equipos (hardware) | 9 |
| [E14] Escapes de información | 8 |
| [A30] Ingeniería social (picaresca) | 8 |
| [E21] Errores de mantenimiento / actualización de programas (software) | 8 |
| [A11] Acceso no autorizado | 7 |
| [E19] Fugas de información | 7 |
| [E24] Caída del sistema por agotamiento de recursos | 7 |
| [A14] Interceptación de información (escucha) | 6 |
| [A4] Manipulación de la configuración | 6 |
| [I10] Degradación de los soportes de almacenamiento de la información | 5 |
| [A26] Ataque destructivo | 5 |
| [A25] Robo | 5 |
| [A18] Destrucción de información | 5 |
| [A5] Suplantación de la identidad del usuario | 5 |
| [A19] Divulgación de información | 5 |
| [A24] Denegación de servicio | 4 |
| [I7] Condiciones inadecuadas de temperatura o humedad | 4 |
| A24] Denegación de servicio | 4 |
| [A12] Análisis de tráfico | 3 |
| [E8] Difusión de software dañino | 3 |
| [I9] Interrupción de otros servicios y suministros esenciales | 3 |
| [A7] Uso no previsto | 3 |
| [A13] Repudio | 1 |
| [A23] Manipulación de los equipos | 1 |
| [E3] Errores de monitorización (log) | 1 |
| [A3] Manipulación de los registros de actividad (log) | 1 |
| **TOTAL** | **291** |

Cuando un activo es blanco de una amenaza es necesario dar una valoración a esta dependiendo del tipo de afectación que puede causar en cada una de sus dimensiones. La mayoría de las veces la amenaza no afecta todas las cinco dimensiones del activo, y si afecta varias no las afecta de la misma manera ni en la

misma cuantía. Una vez identificadas las amenazas el siguiente paso es determinar el nivel de degradación (Cuán afectado resulta el activo) y la probabilidad de ocurrencia (probabilidad de que se materialice la amenaza).

En el análisis desarrollado, esta calificación se da del uno (1) al cinco (5), en el ítem identificado como "Probabilidad de vulneración". Cada uno de los valores cualitativos de la escala de vulneración se traduce a un valor numérico, a saber, 1 "muy raro", 2 "poco probable", 3 "posible", 4 "probable", 5 "prácticamente seguro", de esta manera se calcula el riesgo neto, cuya fórmula es "Valoración del riesgo del activo **x** probabilidad de vulneración".

Del valor del riesgo neto se desprende la criticidad neta, que es la representación de cuán critica es la amenaza identificada frente al activo de infraestructura tecnológica, y se cuantifica con la escala: “1 a 4 despreciable (d)”, “5 a 9 baja (B)”, “10 a 15 apreciable (a)”, “16 a 20 importante (i)” y “21 o mayor crítico(C)”. En el análisis realizado a Kappa10, el cuadro de criticidad neta quedó como se ve en la tabla 12 “Cantidad de amenazas por criticidad neta”, mostrando así que la mayoría de las amenazas de la empresa son Criticas o importantes:

Tabla 12 Cantidad de amenazas por criticidad neta.

| Tipo de criticidad neta | Cantidad de ocurrencias |
|---|---|
| [C] Critico | 164 |
| [I] Importante | 50 |
| [A] Apreciable | 21 |
| [B] Bajo | 39 |
| [D] Despreciable | 17 |
| **TOTAL** | **291** |

De acuerdo con los valores de la tabla 11 se establece el impacto (La cantidad de daño del activo ocurrido por la materialización de una amenaza[61]) de cada una de las amenazas sobre los activos de infraestructura tecnológica. En la tabla 13 “Mapa

[61] GOBIERNO DE ESPAÑA. MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro 1. [2012]. Op. cit. p. 28.

de calor impacto de amenazas" se ve la clasificación de las 291 amenazas de acuerdo con su nivel de impacto sin tratamiento.

Tabla 13 Mapa de calor impacto de amenazas.

| | | IMPACTO | | | | |
|---|---|---|---|---|---|---|
| | | **Insignificante** | **Menor** | **Moderado** | **Mayor** | **Catastrófico** |
| **IMPACTO** | **c** | R1, R3, R9, R22, R29, R30, R121, R125, R126, R127, R129, R161, R162, R167, R168, R185, R189, R190, R192, R193, R195, R207, R212, R214, R215, R217, R224, R229, R234, R235, R236, R241, R246, R247, R268, R271, R272, R273, R275 | R5, R8, R10, R15, R18, R20, R21, R23, R24, R25, R28, R60, R62, R67, R70, R72, R77, R5, R92, R93, R94, R97, R104, R105, R109, R110, R115, R117, R120, R122, R124, R128, R130, R132, R134, R138, R140, R157, R159, R160, R163, R164, R165, R166, R169, R170, R171, R186, R188, R191, R194, R197, R199, R202, R205, R208, R210, R213, R216, R226, R228, R231, R232, R233, R238, R240, R243, R244, R245, R260, R261, R264, R265, R270, R274, R278, R282 | R2, R4, R7, R12, R14, R17, R26, R27, R33, R43, R61, R68, R71, R78, R91, R98, R101, R102, R112, R113, R123, R133, R142, R143, R144, R152, R153, R158, R187, R198, R209, R219, R220, R225, R227, R230, R237, R239, R242, R259, R263, R269, R277, R285 | R6, R16 | |
| | **i** | R11, R13, R19, R59, R63, R64, R65, R66, R69, R73, R74, R75, R76, R89, R95, R96, R99, R100, R103, R106, R107, R108, R111, R114, R116, R118, R119, R131, R135, R136, R137, R139, R151, R154, R155, R156, R276, R279, R280, R281, R283 | R34, R37, R39, R44, R47, R49, R145, R147 | R249 | | |
| | **a** | R196, R200, R201, R203, R204, R206, R258, R262, R266, R267 | R248, R250, R253, R254, R256, R257, R286, R288, R289 | R84, R174 | | |
| | **b** | R31, R32, R35, R36, R38, R40, R41, R42, R45, R46, R48, R50, R141, R146, R148, R149, R150, R31, R221, R222, R223, R251, R252, R255, R284, R287, R290, R291 | R52, R53, R54, R57, R79, R80, R82, R85, R86, R88, R175 | | | |
| | **d** | R51, R55, R56, R58, R81, R83, R87, R173, R176, R177, R178, R179, R180, R181, R182, R183, R184 | | | | |
| **RIESGO** | | **1** | **2** | **3** | **4** | **5** |
| | | **PROBABILIDAD** | | | | |

Una vez identificado el riesgo, la criticidad neta y el impacto de cada amenaza, es necesario comenzar a averiguar qué salvaguardas o controles implementados en la empresa con respecto de cada una de estas, y ver en qué estado de madurez se encuentran, lo que comprende verificar si se están o no poniendo en práctica para mitigar las amenazas. Este proceso de identificación de salvaguardas se realizó mediante reuniones y entrevistas con las áreas encargadas.

Los controles de cada amenaza pueden ser uno o varios, dependiendo de la criticidad de esta y de su forma, pero van definidos en consonancia con la norma ISO 27002[62], en la cual se clasifican de forma ordenada en 14 dominios subdivididos en 35 objetivos de control, que a su vez contienen los 114 controles aplicables. La organización de los controles de la norma se ve en la tabla 14 "Controles ISO 27002":

Tabla 14 Controles ISO 27002.[63]

| CLASE | NOMBRE |
|---|---|
| **Dominio** | **5. POLÍTICAS DE SEGURIDAD.** |
| **Obj. De control** | ***5.1 Directrices de la Dirección en seguridad de la información.*** |
| Control | 5.1.1 Conjunto de políticas para la seguridad de la información. |
| Control | 5.1.2 Revisión de las políticas para la seguridad de la información. |
| **Dominio** | **6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.** |
| **Obj. De control** | ***6.1 Organización interna.*** |
| Control | 6.1.1 Asignación de responsabilidades para la segur. de la información. |
| Control | 6.1.2 Segregación de tareas. |
| Control | 6.1.3 Contacto con las autoridades. |
| Control | 6.1.4 Contacto con grupos de interés especial. |
| Control | 6.1.5 Seguridad de la información en la gestión de proyectos. |
| **Obj. De control** | ***6.2 Dispositivos para movilidad y teletrabajo.*** |
| Control | 6.2.1 Política de uso de dispositivos para movilidad. |
| Control | 6.2.2 Teletrabajo. |
| **Dominio** | **7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.** |
| **Obj. De control** | ***7.1 Antes de la contratación.*** |
| Control | 7.1.1 Investigación de antecedentes. |
| Control | 7.1.2 Términos y condiciones de contratación. |
| **Obj. De control** | ***7.2 Durante la contratación.*** |
| Control | 7.2.1 Responsabilidades de gestión. |
| Control | 7.2.2 Concienciación, educación y capacitación en segur. de la información. |
| Control | 7.2.3 Proceso disciplinario. |
| **Obj. De control** | ***7.3 Cese o cambio de puesto de trabajo.*** |
| Control | 7.3.1 Cese o cambio de puesto de trabajo. |
| **Dominio** | **8. GESTIÓN DE ACTIVOS.** |
| **Obj. De control** | ***8.1 Responsabilidad sobre los activos.*** |
| Control | 8.1.1 Inventario de activos. |

[62] ICONTEC. ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES. Op. cit. p. 1.
[63] Ibíd.

Tabla 14. (Continuación)

| | |
|---|---|
| Control | 8.1.2 Propiedad de los activos. |
| Control | 8.1.3 Uso aceptable de los activos. |
| Control | 8.1.4 Devolución de activos. |
| **Obj. De control** | ***8.2 Clasificación de la información.*** |
| Control | 8.2.1 Directrices de clasificación. |
| Control | 8.2.2 Etiquetado y manipulado de la información. |
| Control | 8.2.3 Manipulación de activos. |
| **Obj. De control** | ***8.3 Manejo de los soportes de almacenamiento.*** |
| Control | 8.3.1 Gestión de soportes extraíbles. |
| Control | 8.3.2 Eliminación de soportes. |
| Control | 8.3.3 Soportes físicos en tránsito. |
| **Dominio** | **9. CONTROL DE ACCESOS.** |
| **Obj. De control** | ***9.1 Requisitos de negocio para el control de accesos.*** |
| Control | 9.1.1 Política de control de accesos. |
| Control | 9.1.2 Control de acceso a las redes y servicios asociados. |
| **Obj. De control** | ***9.2 Gestión de acceso de usuario.*** |
| Control | 9.2.1 Gestión de altas/bajas en el registro de usuarios. |
| Control | 9.2.2 Gestión de los derechos de acceso asignados a usuarios. |
| Control | 9.2.3 Gestión de los derechos de acceso con privilegios especiales. |
| Control | 9.2.4 Gestión de información confidencial de autenticación de usuarios. |
| Control | 9.2.5 Revisión de los derechos de acceso de los usuarios. |
| Control | 9.2.6 Retirada o adaptación de los derechos de acceso |
| **Obj. De control** | ***9.3 Responsabilidades del usuario.*** |
| Control | 9.3.1 Uso de información confidencial para la autenticación. |
| **Obj. De control** | ***9.4 Control de acceso a sistemas y aplicaciones.*** |
| Control | 9.4.1 Restricción del acceso a la información. |
| Control | 9.4.2 Procedimientos seguros de inicio de sesión. |
| Control | 9.4.3 Gestión de contraseñas de usuario. |
| Control | 9.4.4 Uso de herramientas de administración de sistemas. |
| Control | 9.4.5 Control de acceso al código fuente de los programas |
| **Dominio** | **10. CIFRADO.** |
| **Obj. De control** | ***10.1 Controles criptográficos.*** |
| Control | 10.1.1 Política de uso de los controles criptográficos. |
| Control | 10.1.2 Gestión de claves. |
| **Dominio** | **11. SEGURIDAD FÍSICA Y AMBIENTAL.** |
| **Obj. De control** | ***11.1 Áreas seguras.*** |
| Control | 11.1.1 Perímetro de seguridad física. |
| Control | 11.1.2 Controles físicos de entrada. |
| Control | 11.1.3 Seguridad de oficinas, despachos y recursos. |
| Control | 11.1.4 Protección contra las amenazas externas y ambientales. |
| Control | 11.1.5 El trabajo en áreas seguras. |
| Control | 11.1.6 Áreas de acceso público, carga y descarga. |
| **Obj. De control** | ***11.2 Seguridad de los equipos.*** |
| Control | 11.2.1 Emplazamiento y protección de equipos. |
| Control | 11.2.2 Instalaciones de suministro. |
| Control | 11.2.3 Seguridad del cableado. |
| Control | 11.2.4 Mantenimiento de los equipos. |
| Control | 11.2.5 Salida de activos fuera de las dependencias de la empresa. |
| Control | 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones. |
| Control | 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento. |
| Control | 11.2.8 Equipo informático de usuario desatendido. |
| Control | 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla. |
| **Dominio** | **12. SEGURIDAD EN LA OPERATIVA.** |
| **Obj. De control** | ***12.1 Responsabilidades y procedimientos de operación.*** |
| Control | 12.1.1 Documentación de procedimientos de operación. |
| Control | 12.1.2 Gestión de cambios. |
| Control | 12.1.3 Gestión de capacidades. |
| Control | 12.1.4 Separación de entornos de desarrollo, prueba y producción. |
| **Obj. De control** | ***12.2 Protección contra código malicioso.*** |
| Control | 12.2.1 Controles contra el código malicioso. |
| **Obj. De control** | ***12.3 Copias de seguridad.*** |
| Control | 12.3.1 Copias de seguridad de la información. |

Tabla 14. (Continuación)

| | |
|---|---|
| **Obj. De control** | ***12.4 Registro de actividad y supervisión.*** |
| Control | 12.4.1 Registro y gestión de eventos de actividad. |
| Control | 12.4.2 Protección de los registros de información. |
| Control | 12.4.3 Registros de actividad del administrador y operador del sistema. |
| Control | 12.4.4 Sincronización de relojes. |
| **Obj. De control** | ***12.5 Control del software en explotación.*** |
| Control | 12.5.1 Instalación del software en sistemas en producción. |
| **Obj. De control** | ***12.6 Gestión de la vulnerabilidad técnica.*** |
| Control | 12.6.1 Gestión de las vulnerabilidades técnicas. |
| Control | 12.6.2 Restricciones en la instalación de software. |
| **Obj. De control** | ***12.7 Consideraciones de las auditorías de los sistemas de información.*** |
| Control | 12.7.1 Controles de auditoría de los sistemas de información. |
| **Dominio** | **13. SEGURIDAD EN LAS TELECOMUNICACIONES.** |
| **Obj. De control** | ***13.1 Gestión de la seguridad en las redes.*** |
| Control | 13.1.1 Controles de red. |
| Control | 13.1.2 Mecanismos de seguridad asociados a servicios en red. |
| Control | 13.1.3 Segregación de redes. |
| **Obj. De control** | ***13.2 Intercambio de información con partes externas.*** |
| Control | 13.2.1 Políticas y procedimientos de intercambio de información. |
| Control | 13.2.2 Acuerdos de intercambio. |
| Control | 13.2.3 Mensajería electrónica. |
| Control | 13.2.4 Acuerdos de confidencialidad y secreto |
| **Dominio** | **14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.** |
| **Obj. De control** | ***14.1 Requisitos de seguridad de los sistemas de información.*** |
| Control | 14.1.1 Análisis y especificación de los requisitos de seguridad. |
| Control | 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas. |
| Control | 14.1.3 Protección de las transacciones por redes telemáticas. |
| **Obj. De control** | ***14.2 Seguridad en los procesos de desarrollo y soporte.*** |
| Control | 14.2.1 Política de desarrollo seguro de software. |
| Control | 14.2.2 Procedimientos de control de cambios en los sistemas. |
| Control | 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo. |
| Control | 14.2.4 Restricciones a los cambios en los paquetes de software. |
| Control | 14.2.5 Uso de principios de ingeniería en protección de sistemas. |
| Control | 14.2.6 Seguridad en entornos de desarrollo. |
| Control | 14.2.7 Externalización del desarrollo de software. |
| Control | 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas. |
| Control | 14.2.9 Pruebas de aceptación. |
| **Obj. De control** | ***14.3 Datos de prueba.*** |
| Control | 14.3.1 Protección de los datos utilizados en pruebas. |
| **Dominio** | **15. RELACIONES CON SUMINISTRADORES.** |
| **Obj. De control** | ***15.1 Seguridad de la información en las relaciones con suministradores.*** |
| Control | 15.1.1 Política de seguridad de la información para suministradores. |
| Control | 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores. |
| Control | 15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones. |
| **Obj. De control** | ***15.2 Gestión de la prestación del servicio por suministradores.*** |
| Control | 15.2.1 Supervisión y revisión de los servicios prestados por terceros. |
| Control | 15.2.2 Gestión de cambios en los servicios prestados por terceros. |
| **Dominio** | **16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.** |
| **Obj. De control** | ***16.1 Gestión de incidentes de seguridad de la información y mejoras.*** |
| Control | 16.1.1 Responsabilidades y procedimientos. |
| Control | 16.1.2 Notificación de los eventos de seguridad de la información. |
| Control | 16.1.3 Notificación de puntos débiles de la seguridad. |
| Control | 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones. |
| Control | 16.1.5 Respuesta a los incidentes de seguridad. |
| Control | 16.1.6 Aprendizaje de los incidentes de seguridad de la información. |
| Control | 16.1.7 Recopilación de evidencias. |
| **Dominio** | **17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.** |
| **Obj. De control** | ***17.1 Continuidad de la seguridad de la información.*** |
| Control | 17.1.1 Planificación de la continuidad de la seguridad de la información. |
| Control | 17.1.2 Implantación de la continuidad de la seguridad de la información. |

Tabla 14. (Continuación)

| | |
|---|---|
| Control | 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información. |
| **Obj. De control** | ***17.2 Redundancias.*** |
| Control | 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información. |
| **Dominio** | **18. CUMPLIMIENTO.** |
| **Obj. De control** | ***18.1 Cumplimiento de los requisitos legales y contractuales.*** |
| Control | 18.1.1 Identificación de la legislación aplicable. |
| Control | 18.1.2 Derechos de propiedad intelectual (DPI). |
| Control | 18.1.3 Protección de los registros de la organización. |
| Control | 18.1.4 Protección de datos y privacidad de la información personal. |
| Control | 18.1.5 Regulación de los controles criptográficos. |
| **Obj. De control** | ***18.2 Revisiones de la seguridad de la información.*** |
| Control | 18.2.1 Revisión independiente de la seguridad de la información. |
| Control | 18.2.2 Cumplimiento de las políticas y normas de seguridad. |
| Control | 18.2.3 Comprobación del cumplimiento. |

Actualmente Kappa10 Ltda. cuenta con controles implementados debidamente documentados, controles implementados sin documentar, y algunas amenazas que no tienen control, por lo que su nivel de impacto no cambiará frente al nivel de impacto residual.

Una vez confirmados y documentados los controles actuales y su nivel de efectividad frente a las amenazas, vuelven a clasificarse de acuerdo con su nuevo impacto, el impacto residual. Del valor del riesgo residual, obtenido de la división del riesgo neto entre la calidad de la gestión de la amenaza, se desprende la criticidad residual, que se cuantifica con la misma escala de la criticidad neta, a saber: “1 a 4 despreciable (d)”, “5 a 9 baja (b)”, “10 a 15 apreciable (a)”, “16 a 20 importante (i)” y “21 o mayor crítico(C)”. Luego de registrar los datos en la matriz, el resultado se puede ver en la tabla 15 “Cantidad de amenazas por criticidad residual”:

Tabla 15 Cantidad de amenazas por criticidad residual.

| Tipo de criticidad residual | Cantidad de ocurrencias |
|---|---|
| [C] Critico | 31 |
| [I] Importante | 11 |
| [A] Apreciable | 68 |
| [B] Bajo | 111 |
| [D] Despreciable | 70 |
| **TOTAL** | **291** |

De acuerdo con los valores de esta tabla se establece el impacto residual, que es el impacto que queda de cada una de las amenazas sobre los activos de

infraestructura tecnológica después de que se ha aplicado un control o salvaguarda. En la tabla 16 “Mapa de calor impacto residual de amenazas” se muestra la clasificación de las 291 amenazas de acuerdo con su nivel de impacto residual alineado a la matriz de análisis de riesgos.

Tabla 16 Mapa de calor impacto residual de amenazas.

| | | IMPACTO | | | | |
|---|---|---|---|---|---|---|
| | | **Insignificante** | **Menor** | **Moderado** | **Mayor** | **Catastrófico** |
| **IMPACTO** | **c** | R275, R273, R272, R271, R268, R247, R246, R241, R236, R235, R234, R229, R224, R217, R215, R214, R212, R211, R207, R195, R193, R192, R190, R189, R185, R168, R167, R162, R161, R129, R127, R126, R125, R121, R30, R29, R22, R9, R3, R1 | R282, R278, R274, R270, R265, R264, R261, R260, R245, R244, R243, R240, R238, R233, R232, R231, R228, R226, R216, R213, R210, R208, R205, R202, R199, R197, R194, R191, R188, R186, R172, R171, R170, R169, R166, R165, R164, R163, R160, R159, R157, R140, R138, R134, R132, R130, R128, R124, R122, R120, R117, R115, R110, R109, R105, R104, R97, R94, R93, R92, R90, R77, R72, R70, R67, R62, R60, R28, R25, R24, R23, R21, R20, R18, R15, R10, R8, R5 | R285, R277, R269, R263, R259, R242, R239, R237, R230, R227, R225, R220, R219, R209, R198, R187, R158, R153, R152, R144, R143, R142, R133, R123, R113, R112, R102, R101, R98, R91, R78, R71, R68, R61, R43, R33, R27, R26, R17, R14, R12, R7, R4, R2 | R16, R6 | N/A |
| | i | N/A | R147, R145, R47, R37 | R249 | N/A | N/A |
| | a | N/A | R289, R288, R286 | R84 | N/A | N/A |
| | **b** | N/A | N/A | N/A | N/A | N/A |
| | **d** | N/A | N/A | N/A | N/A | N/A |
| **RIESGO** | | **1** | **2** | **3** | **4** | **5** |
| | | **PROBABILIDAD** | | | | |

En conformidad con lo expresado en el mapa de calor del impacto residual, la decisión de la empresa, de acuerdo con el alcance del proyecto, es que se proponga un posible plan de tratamiento de riesgos (PTR) para mitigar, transferir, aceptar o eliminar, los riesgos con una calificación de “nivel de aceptación del riesgo” que sea inaceptable. Esta decisión basada en los recursos y la premura que representa cada amenaza frente al objetivo del proyecto y las metas de la empresa permitió generar un PTR adecuado que se presentará en el siguiente aparte.

### 6.2.3 Plan de tratamiento de riesgos sugerido para Kappa10

La gestión del riesgo es el conjunto de decisiones que debe tomarse de acuerdo con el nivel de exposición del sistema de la organización al riesgo y el impacto detectados. Estas decisiones pueden basarse en criterios como la gravedad del impacto, las responsabilidades legales a las que está sometida la organización, las obligaciones reglamentarias del sector, y las obligaciones contractuales que tiene la organización. Además de las mencionadas hay otras razones, dentro de las cuales se encuentra la posibilidad de acceso a certificaciones reconocidas de seguridad, que es el caso de Kappa10.

El tratamiento del riesgo va de la mano con la dirección de la organización, es decir, quien toma finalmente la decisión de dar un control a cada riesgo. Hay dos opciones en cuanto a este tema, la primera es disminuir el riesgo residual (aceptar un menor riesgo), y la segunda es incrementar el riesgo residual (aceptar un mayor riesgo). Estas decisiones se basan en la calificación del riesgo de acuerdo con el análisis que se esté realizando, así como en el coste total que por ejemplo comprende la compra de nuevas salvaguardas para disminuir el riesgo residual.

Durante el plan de tratamiento de riesgos deben tenerse en cuenta las opciones frente a los riesgos, las cuales pueden identificarse como: eliminación, mitigación, compartición y financiación. Es primordial entender lo que significa cada una de estas opciones, ya que son las que se utilizarán durante esta fase, por lo tanto, a continuación, se explica brevemente cada una de estas.

- Eliminación: supone que se prescinda de algún activo e información que este proporcione, algo que no es muy común, pero sirve para quitar el riesgo relacionado de raíz.
- Mitigación: en esta se puede optar por dos opciones, aminorar la degradación que causa la amenaza, o reducir su probabilidad de ocurrencia, ambas se realizan mediante controles o salvaguardas implementadas.

- Compartición o "transferencia del riesgo": Es precisamente delegar las responsabilidades técnicas y legales de un sistema a un tercero.
- Financiación: es cuando se acepta un riesgo, lo que hace que la organización deba reservar ciertos fondos en caso de que dicho riesgo llegase a concretarse, dado que se debería responder por las consecuencias. En algunos casos las organizaciones llaman a esta reserva el “fondo de contingencia”.

Teniendo presentes los conceptos de gestión del riesgo analizados previamente, y con ayuda de la “Matriz de análisis de riesgos Kappa10.xlsx”, se definieron los controles para los riesgos residuales “inaceptables” en conjunto con las áreas de operaciones y conformidad de la empresa, arrojando como resultado el siguiente análisis:

- Se encontraron 69 riesgos residuales de nivel inaceptable durante el análisis de riesgos realizado.
- Los 69 riesgos encontrados se dividen por los siguientes tipos de activos:
    - [HW] EQUIPAMENTO INFORMÁTICO: 33
    - [SW] SOFTWARE: 24
    - [D] DATOS: 6
    - [S] SERVICIOS: 3
    - [AUX] EQUIPAMENTO AUXILIAR: 3
- De los 69 riesgos encontrados, 59 ya tienen un control actualmente, pero este no es efectivo o no se encuentra en un nivel de madurez aceptable que permita mitigar el riesgo.
- En este caso particular la organización ha decidido realizar el análisis de riesgos para cumplir los requerimientos que exige la certificación ISO 27001:2013[64], y no como un requisito legal o contractual, lo que deja un mayor margen de ejecución de labores en el plan de tratamiento del riesgo.
- De los 69 riesgos se mitigarán 61, se aceptarán 8 y se transferirá 1. Dentro del aparte de recomendaciones se indicarán los pasos que se recomienda tomar a

[64] ICONTEC. Op. Cit., p. 1.

Kappa 10 frente al análisis realizado en cuanto a la mitigación transferencia y aceptación de riesgos.

A continuación, en la tabla 17 “Plan de tratamiento de riesgos (PTR) Kappa10” se muestra en detalle el plan de tratamiento que se sugiere a cada riesgo residual inaceptable encontrado durante el proceso:

Tabla 17 Plan de tratamiento de riesgos (PTR) Kappa10[65].

| Activo | Amenaza MAGERIT | Plan de tratamiento de riesgos | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | Transferi | Aceptar | Mitigar | Nomenclatura del control | Control | Descripción del control | Descripción de aplicación del control |
| [HW_FORTIWIFI_60D-POE] | [A24] Denegación de servicio | | | X | A12.1.3 | Gestión de capacidad | Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema. | Gestión de capacidad monitoreada mediante el software PRTG, el cual estará productivo dentro de los siguientes 30 días. |
| [HW_FORTIWIFI_60D-POE] | [E15] Alteración accidental de la información | | | X | A12.3.1 | Respaldo de la información | Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas. | Se realizan copias mensuales de la configuración del dispositivo. Adicionalmente se deben realizar copias previas y posteriores a cada cambio de configuración, las cuales se guardan en un repositorio de Google Drive. |
| [HW_FORTIWIFI_60D-POE] | [E18] Destrucción de información | | | X | A12.3.1 | Respaldo de la información | Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas. | Se realizan copias mensuales de la configuración del dispositivo. Adicionalmente se deben realizar copias previas y posteriores a cada cambio de configuración, las cuales se guardan en un repositorio de Google Drive. |

[65] UNAD. Op. Cit., p. 8.

Tabla 17. (Continuación)

| Activo | Amenaza MAGERIT | Plan de tratamiento de riesgos | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | Transferir | Aceptar | Mitigar | Nomenclatura del control | Control | Descripción del control | Descripción de aplicación del control |
| [HW_FORTIWIFI_60D-POE] | [A5] Suplantación de la identidad del usuario | | | X | A9.2.2 | Suministro de acceso de usuarios | Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios. | Implementación de la plataforma FortiAuthenticator, la cual estará enlazada al controlador de dominio de la red de Kappa10. |
| [HW_FORTIWIFI_60D-POE] | [A6] Abuso de privilegios de acceso | | | X | A9.2.3 | Gestión de derechos de acceso privilegiado | Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado | Implementación de la plataforma FortiAuthenticator, la cual estará enlazada al controlador de dominio de la red de Kappa10, el cual maneja los diferentes grupos de trabajo a los cuales se les otorgarán privilegios de acuerdo con cada rol. |
| [HW_FORTIWIFI_60D-POE] | [A11] Acceso no autorizado | | | X | A9.1.1 | Política de control de acceso | Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la seguridad de la información. | Se debe implementar un sistema de autenticación que soporte el uso único de usuario y contraseña para acceder a la administración de la plataforma que contiene información susceptible de la compañía. |

Tabla 17. (Continuación)

| Activo | Amenaza MAGERIT | Plan de tratamiento de riesgos | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | Transferir | Aceptar | Mitigar | Nomenclatura del control | Control | Descripción del control | Descripción de aplicación del control |
| [HW_FORTIWIFI_60D-POE] | [E2] Errores del administrador | | | X | A.14.2.2 | Procedimientos de control de cambios en sistemas | Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios. | Procedimiento de TI llamado "Ventanas de mantenimiento". De acuerdo con este se debe solicitar permisos para ejecución del cambio en un horario establecido, si el cambio no es exitoso, debe realizarse rollback. Todo debe quedar documentado en el repositorio de Kappa10. |
| [HW_FORTIGATE_60D] | [A24] Denegación de servicio | | | X | A12.1.3 | Gestión de capacidad | Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema. | Gestión de capacidad monitoreada mediante el software PRTG, el cual estará productivo dentro de los siguientes 30 días. |
| [HW_FORTIGATE_60D] | [E15] Alteración accidental de la información | | | X | A12.3.1 | Respaldo de la información | Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas. | Se realizan copias mensuales de la configuración del dispositivo. Adicionalmente se deben realizar copias previas y posteriores a cada cambio de configuración, las cuales se guardan en un repositorio de Google Drive. |
| [HW_FORTIGATE_60D] | [A5] Suplantación de la identidad del usuario | | | X | A9.2.2 | Suministro de acceso de usuarios | Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios. | Implementación de la plataforma FortiAuthenticator, la cual estará enlazada al controlador de dominio de la red de Kappa10. |

Tabla 17. (Continuación)

| Activo | Amenaza MAGERIT | Plan de tratamiento de riesgos | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | Transferir | Aceptar | Mitigar | Nomenclatura del control | Control | Descripción del control | Descripción de aplicación del control |
| [HW_FORTIGATE_60D] | [A6] Abuso de privilegios de acceso | | | X | A9.2.3 | Gestión de derechos de acceso privilegiado | Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado | Implementación de la plataforma FortiAuthenticator, la cual estará enlazada al controlador de dominio de la red de Kappa10, el cual maneja los diferentes grupos de trabajo a los cuales se les otorgarán privilegios de acuerdo con cada rol. |
| [D_DOMAIN_CONTROLLER] | [E19] Fugas de información | | | X | A9.2.3 | Gestión de derechos de acceso privilegiado | Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado | El acceso es brindado de acuerdo con el rol, y únicamente por el administrador del controlador de dominio. |
| [D_DOMAIN_CONTROLLER] | [E15] Alteración accidental de la información | | | X | A12.3.1 | Respaldo de la información | Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas. | Se realiza backup semanal del controlador de dominio. |
| [D_DOMAIN_CONTROLLER] | [E18] Destrucción de información | | | X | A12.3.1 | Respaldo de la información | Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas. | Se realiza backup semanal del controlador de dominio. |

Tabla 17. (Continuación)

| Activo | Amenaza MAGERIT | Plan de tratamiento de riesgos | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | Transferir | Aceptar | Mitigar | Nomenclatura del control | Control | Descripción del control | Descripción de aplicación del control |
| [D_DOMAIN_CONTROLLER] | [A5] Suplantación de la identidad del usuario | | | X | A7.2.2 | Toma de conciencia, educación y formación en la seguridad de la información. | Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo. | Se dictarán capacitaciones sobre seguridad informática dentro de la empresa, para evitar cosas como fraudes, configuraciones débiles, etc. |
| [D_DOMAIN_CONTROLLER] | [A6] Abuso de privilegios de acceso | | | X | A9.2.3 | Gestión de derechos de acceso privilegiado | Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado | El acceso es brindado de acuerdo con el rol, y únicamente por el administrador del controlador de dominio. |
| [D_DOMAIN_CONTROLLER] | [A11] Acceso no autorizado | | | X | A9.1.1 | Política de control de acceso | Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la seguridad de la información. | Se debe implementar un sistema de autenticación que soporte el uso único de usuario y contraseña para acceder a la administración de la plataforma que contiene información susceptible de la compañía. |
| [AUX_CAMARA-OF503] | [I6] Corte del suministro eléctrico | | X | | | | | Se decide aceptar el riesgo por parte de la compañía por el momento, ya que se está enfocando a los empleados y al SGSI, a la mitigación de los riesgos más críticos para el negocio y para la consecución de la certificación ISO 27001:2013. |

Tabla 17. (Continuación)

| Activo | Amenaza MAGERIT | Plan de tratamiento de riesgos | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | Transferir | Aceptar | Mitigar | Nomenclatura del control | Control | Descripción del control | Descripción de aplicación del control |
| [AUX_CAMARA-OF211] | [I6] Corte del suministro eléctrico | | X | | | | | Se decide aceptar el riesgo por parte de la compañía por el momento, ya que se está enfocando a los empleados y al SGSI, a la mitigación de los riesgos más críticos para el negocio y para la consecución de la certificación ISO 27001:2013. |
| [HW_FORTIAP_211B] | [I6] Corte del suministro eléctrico | | X | | | | | Se decide aceptar el riesgo por parte de la compañía por el momento, ya que se está enfocando a los empleados y al SGSI, a la mitigación de los riesgos más críticos para el negocio y para la consecución de la certificación ISO 27001:2013. |
| [HW_FORTIAP_211B] | [A14] Interceptación de información (escucha) | | | X | A11.2.1 | Ubicación y protección de los equipos | Los equipos deben de estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado. | Las redes inalámbricas se encuentran ocultas, adicionalmente la potencia de irradiación de los AP se encuentra restringida a la zona de la oficina. |
| [HW_FORTIAP_PU423E] | [I6] Corte del suministro eléctrico | | | X | A11.2.2 | Servicios de suministro | Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro. | El AP se encuentra conectado por POE al equipo FortiWifi60D de la oficina 503, que se encuentra alimentado y protegido mediante la UPS PRO1500. |

Tabla 17. (Continuación)

| Activo | Amenaza MAGERIT | Plan de tratamiento de riesgos | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | Transferir | Aceptar | Mitigar | Nomenclatura del control | Control | Descripción del control | Descripción de aplicación del control |
| [HW_FORTIAP_PU423E] | [A14] Interceptación de información (escucha) | | | X | A11.2.1 | Ubicación y protección de los equipos | Los equipos deben de estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado. | Las redes inalámbricas se encuentran ocultas, adicionalmente la potencia de irradiación de los AP se encuentra restringida a la zona de la oficina. |
| [HW_TELEFONO_IP_RECEP.] | [I6] Corte del suministro eléctrico | | X | | | | | Se decide aceptar el riesgo por parte de la compañía por el momento, ya que se está enfocando a los empleados y al SGSI, a la mitigación de los riesgos más críticos para el negocio y para la consecución de la certificación ISO 27001:2013. |
| [HW_TELEFONO_IP_RECEP.] | [I9] Interrupción de otros servicios y suministros esenciales | | X | | | | | Se decide aceptar el riesgo por parte de la compañía por el momento, ya que se está enfocando a los empleados y al SGSI, a la mitigación de los riesgos más críticos para el negocio y para la consecución de la certificación ISO 27001:2013. |
| [HW_SWITCH_CATALYST_2960] | [I5] Avería de origen físico o lógico | | | X | A11.2.1 | Ubicación y protección de los equipos | Los equipos deben de estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado. | El dispositivo se encuentra protegido mediante la UPS PRO1500 y el rack de la oficina 503. |

Tabla 17. (Continuación)

| Activo | Amenaza MAGERIT | Plan de tratamiento de riesgos | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | Transferir | Aceptar | Mitigar | Nomenclatura del control | Control | Descripción del control | Descripción de aplicación del control |
| [HW_PBX_UCM6104] | [I5] Avería de origen físico o lógico | | | X | A11.2.1 | Ubicación y protección de los equipos | Los equipos deben de estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado. | El dispositivo se encuentra protegido mediante la UPS PRO1500 y el rack de la oficina 503. |
| [HW_MODEM_ISP_OF503] | [I6] Corte del suministro eléctrico | | | X | A11.2.2 | Servicios de suministro | Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro. | El dispositivo se conectará a la UPS PRO1500 para evitar fallas en su sistema. |
| [HW_MODEM_ISP_OF503] | [I8] Fallo de servicios de comunicaciones | X | | | A15.1.3 | Cadena de suministro de tecnología de información y comunicación | Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación. | Se transfiere la responsabilidad al ISP (ETB) en concordancia con los acuerdos del contrato. |
| [HW_MODEM_ISP_OF211] | [I6] Corte del suministro eléctrico | | | X | A11.2.2 | Servicios de suministro | Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro. | El dispositivo se encuentra conectado a la UPS GALLEON para evitar fallas en su sistema. |

Tabla 17. (Continuación)

| Activo | Amenaza MAGERIT | Plan de tratamiento de riesgos | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | Transferir | Aceptar | Mitigar | Nomenclatura del control | Control | Descripción del control | Descripción de aplicación del control |
| [AUX_UPS_PRO1500] | [I6] Corte del suministro eléctrico | | X | | | | | Se decide aceptar el riesgo por parte de la compañía por el momento, ya que se está enfocando a los empleados y al SGSI, a la mitigación de los riesgos más críticos para el negocio y para la consecución de la certificación ISO 27001:2013. |
| [SW_VM_FORTIAUTHENTICATOR] | [I5] Avería de origen físico o lógico | | | X | A12.3.1 | Respaldo de la información | Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas. | Se realizarán copias mensuales de la configuración del dispositivo. Adicionalmente se deben realizar copias previas y posteriores a cada cambio de configuración, las cuales se guardan en un repositorio de Google Drive. |
| [SW_VM_FORTIAUTHENTICATOR] | [I6] Corte del suministro eléctrico | | | X | A11.2.2 | Servicios de suministro | Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro. | El dispositivo donde está alojado el servicio se encuentra conectado a la UPS GALLEON para evitar fallas en su sistema. |
| [SW_VM_FORTIAUTHENTICATOR] | [I8] Fallo de servicios de comunicaciones | | | X | A15.1.3 | Cadena de suministro de tecnología de información y comunicación | Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación. | Se validará la compra de un canal de Internet alterno para evitar la pérdida total del servicio. |

Tabla 17. (Continuación)

| Activo | Amenaza MAGERIT | Plan de tratamiento de riesgos | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | Transferir | Aceptar | Mitigar | Nomenclatura del control | Control | Descripción del control | Descripción de aplicación del control |
| [SW_VM_FORTIAUTHENTICATOR] | [I9] Interrupción de otros servicios y suministros esenciales | | | X | A11.2.2 | Servicios de suministro | Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro. | El controlador de dominio es un servicio esencial para el funcionamiento de la gestión de identidad con FortiAuthenticator, por lo que se realizará una réplica de este servicio en la nube como parte del DRP (Plan de Recuperación ante Desastres). |
| [SW_VM_FORTIAUTHENTICATOR] | [E14] Escapes de información | | | X | A9.2.3 | Gestión de derechos de acceso privilegiado | Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado | El acceso es brindado de acuerdo con el rol, y únicamente por el administrador del controlador de dominio, que estará sincronizado con la plataforma. |
| [SW_VM_FORTIAUTHENTICATOR] | [E15] Alteración accidental de la información | | | X | A12.3.1 | Respaldo de la información | Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas. | Se realizarán copias mensuales de la configuración del dispositivo. Adicionalmente se deben realizar copias previas y posteriores a cada cambio de configuración, las cuales se guardan en un repositorio de Google Drive. |
| [SW_VM_FORTIAUTHENTICATOR] | [E19] Fugas de información | | | X | A9.2.3 | Gestión de derechos de acceso privilegiado | Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado | El acceso es brindado de acuerdo con el rol, y únicamente por el administrador del controlador de dominio, que estará sincronizado con la plataforma. |

Tabla 17. (Continuación)

| Activo | Amenaza MAGERIT | Plan de tratamiento de riesgos | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | Transferir | Aceptar | Mitigar | Nomenclatura del control | Control | Descripción del control | Descripción de aplicación del control |
| [SW_VM_FORTIAUTHENTICATOR] | [E21] Errores de mantenimiento / actualización de programas (software) | | | X | A11.2.4 | Mantenimiento de los equipos. | Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas. | El mantenimiento al equipo comprende un reinicio de la máquina host al año, y la actualización del firmware de acuerdo con la compatibilidad de este con las demás plataformas, solo de ser necesario. |
| [SW_VM_FORTIAUTHENTICATOR] | [A3] Manipulación de los registros de actividad (log) | | | X | A12.4.2 | Protección de la información de registro | Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado. | Los registros de los eventos son inalterables, y solo es posible hacer un borrado total de ellos mediante formateo del disco. Adicionalmente, solo se permite hacer esto desde el usuario administrador. También se contará con un repositorio externo a mediano plazo. |
| [SW_VM_FORTIAUTHENTICATOR] | [A5] Suplantación de la identidad del usuario | | | X | A7.2.2 | Toma de conciencia, educación y formación en la seguridad de la información. | Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo. | Se dictarán capacitaciones sobre seguridad informática dentro de la empresa, para evitar cosas como fraudes, configuraciones débiles, etc. |

Tabla 17. (Continuación)

| Activo | Amenaza MAGERIT | Plan de tratamiento de riesgos | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | Transferir | Aceptar | Mitigar | Nomenclatura del control | Control | Descripción del control | Descripción de aplicación del control |
| [SW_VM_FORTIAUTHENTICATOR] | [A6] Abuso de privilegios de acceso | | | X | A9.2.3 | Gestión de derechos de acceso privilegiado | Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado | Implementación de la plataforma FortiAuthenticator, la cual estará enlazada al controlador de dominio de la red de Kappa10, el cual maneja los diferentes grupos de trabajo a los cuales se les otorgarán privilegios de acuerdo con cada rol. |
| [SW_VM_FORTIAUTHENTICATOR] | [A13] Repudio | | | X | A12.4.1 | Registro de eventos | Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información. | Los registros de los eventos son inalterables, y solo es posible hacer un borrado total de ellos mediante formateo del disco. Adicionalmente, solo se permite hacer esto desde el usuario administrador. También se contará con un repositorio externo a mediano plazo. |
| [SW_VM_FORTIAUTHENTICATOR] | [A30] Ingeniería social (picaresca) | | | X | A7.2.2 | Toma de conciencia, educación y formación en la seguridad de la información. | Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo. | Se dictarán capacitaciones sobre seguridad informática dentro de la empresa, para evitar cosas como fraudes, configuraciones débiles, etc. |

Tabla 17. (Continuación)

| Activo | Amenaza MAGERIT | Plan de tratamiento de riesgos | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | Transferir | Aceptar | Mitigar | Nomenclatura del control | Control | Descripción del control | Descripción de aplicación del control |
| [HW_SRV_PRINCIPAL] | [I5] Avería de origen físico o lógico | | | X | A11.2.1 | Ubicación y protección de los equipos | Los equipos deben de estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado. | El dispositivo se encuentra protegido mediante la UPS PRO1500 y el rack de la oficina 503. |
| [HW_SRV_PRINCIPAL] | [I6] Corte del suministro eléctrico | | | X | A11.2.2 | Servicios de suministro | Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro. | El dispositivo se encuentra conectado a la UPS PRO1500 para evitar fallas en su sistema. |
| [HW_SRV_PRINCIPAL] | [I8] Fallo de servicios de comunicaciones | | | X | A15.1.3 | Cadena de suministro de tecnología de información y comunicación | Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación. | Se validará la compra de un canal de Internet alterno para evitar la pérdida total del servicio. |
| [HW_SRV_PRINCIPAL] | [E8] Difusión de software dañino | | | X | A12.2.1 | Controles contra códigos maliciosos | Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos. | Los sistemas se mantendrán parchados y actualizados, con su firewall local en funcionamiento y con su antivirus activo. Adicionalmente, las políticas de UTM de los NGFW también realizarán un control perimetral de las amenazas al dispositivo. |

Tabla 17. (Continuación)

| Activo | Amenaza MAGERIT | Plan de tratamiento de riesgos | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | Transferir | Aceptar | Mitigar | Nomenclatura del control | Control | Descripción del control | Descripción de aplicación del control |
| [HW_SRV_PRINCIPAL] | [A6] Abuso de privilegios de acceso | | | X | A7.2.2 | Toma de conciencia, educación y formación en la seguridad de la información. | Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo. | Se dictarán capacitaciones sobre seguridad informática dentro de la empresa, para evitar cosas como fraudes, configuraciones débiles, etc. |
| [HW_SRV_LABORATORIO] | [I6] Corte del suministro eléctrico | | | X | A11.2.2 | Servicios de suministro | Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro. | El dispositivo se encuentra conectado a la UPS GALLEON para evitar fallas en su sistema. |
| [HW_SRV_CONTABILIDAD] | [I5] Avería de origen físico o lógico | | | X | A11.2.1 | Ubicación y protección de los equipos | Los equipos deben de estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado. | El dispositivo se encuentra protegido mediante la UPS PRO1500 y el rack de la oficina 503. |
| [HW_SRV_CONTABILIDAD] | [I6] Corte del suministro eléctrico | | | X | A11.2.2 | Servicios de suministro | Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro. | El dispositivo se encuentra conectado a la UPS PRO1500 para evitar fallas en su sistema. |

Tabla 17. (Continuación)

| Activo | Amenaza MAGERIT | Plan de tratamiento de riesgos | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | Transferir | Aceptar | Mitigar | Nomenclatura del control | Control | Descripción del control | Descripción de aplicación del control |
| [HW_SRV_CONTABILIDAD] | [I8] Fallo de servicios de comunicaciones | | | X | A15.1.3 | Cadena de suministro de tecnología de información y comunicación | Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación. | Se validará la compra de un canal de Internet alterno para evitar la pérdida total del servicio. |
| [HW_SRV_CONTABILIDAD] | [E8] Difusión de software dañino | | | X | A12.2.1 | Controles contra códigos maliciosos | Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos. | Los sistemas se mantendrán parchados y actualizados, con su firewall local en funcionamiento y con su antivirus activo. Adicionalmente, las políticas de UTM de los NGFW también realizarán un control perimetral de las amenazas al dispositivo. |
| [HW_SRV_CONTABILIDAD] | [A6] Abuso de privilegios de acceso | | | X | A7.2.2 | Toma de conciencia, educación y formación en la seguridad de la información. | Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo. | Se dictarán capacitaciones sobre seguridad informática dentro de la empresa, para evitar cosas como fraudes, configuraciones débiles, etc. |

Tabla 17. (Continuación)

| Activo | Amenaza MAGERIT | Plan de tratamiento de riesgos | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | Transferir | Aceptar | Mitigar | Nomenclatura del control | Control | Descripción del control | Descripción de aplicación del control |
| [SW_ITOP] | [I6] Corte del suministro eléctrico | | | X | A11.2.2 | Servicios de suministro | Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro. | El dispositivo donde está alojado el servicio se encuentra conectado a la UPS PRO1500 para evitar fallas en su sistema. |
| [SW_ITOP] | [I8] Fallo de servicios de comunicaciones | | | X | A15.1.3 | Cadena de suministro de tecnología de información y comunicación | Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación. | Se validará la compra de un canal de Internet alterno para evitar la pérdida total del servicio. |
| [SW_ITOP] | [E1] Errores de los usuarios | | | X | A12.3.1 | Respaldo de la información | Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas. | Se realizan copias de seguridad semanales en el repositorio de Kappa10. |
| [SW_ITOP] | [E14] Escapes de información | | | X | A12.3.1 | Respaldo de la información | Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas. | Se realizan copias de seguridad semanales en el repositorio de Kappa10. |
| [SW_SIIGO] | [I6] Corte del suministro eléctrico | | | X | A11.2.2 | Servicios de suministro | Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro. | El dispositivo donde está alojado el servicio se encuentra conectado a la UPS PRO1500 para evitar fallas en su sistema. |

Tabla 17. (Continuación)

| Activo | Amenaza MAGERIT | Plan de tratamiento de riesgos | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | Transferir | Aceptar | Mitigar | Nomenclatura del control | Control | Descripción del control | Descripción de aplicación del control |
| [SW_SIIGO] | [I8] Fallo de servicios de comunicaciones | | | X | A15.1.3 | Cadena de suministro de tecnología de información y comunicación | Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación. | Se validará la compra de un canal de Internet alterno para evitar la pérdida total del servicio. |
| [SW_SIIGO] | [E1] Errores de los usuarios | | | X | A12.3.1 | Respaldo de la información | Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas. | Se realizan copias de seguridad semanales en el repositorio de Kappa10. |
| [SW_SIIGO] | [E14] Escapes de información | | | X | A12.3.1 | Respaldo de la información | Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas. | Se realizan copias de seguridad semanales en el repositorio de Kappa10. |
| [SW_PRTG] | [I6] Corte del suministro eléctrico | | | X | A11.2.2 | Servicios de suministro | Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro. | El dispositivo donde está alojado el servicio se encuentra conectado a la UPS GALLEON para evitar fallas en su sistema. |
| [SW_PRTG] | [E14] Escapes de información | | | X | A9.2.3 | Gestión de derechos de acceso privilegiado | Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado | El acceso es brindado de acuerdo con el rol, y únicamente por el administrador del controlador de dominio, que estará sincronizado con la plataforma. |

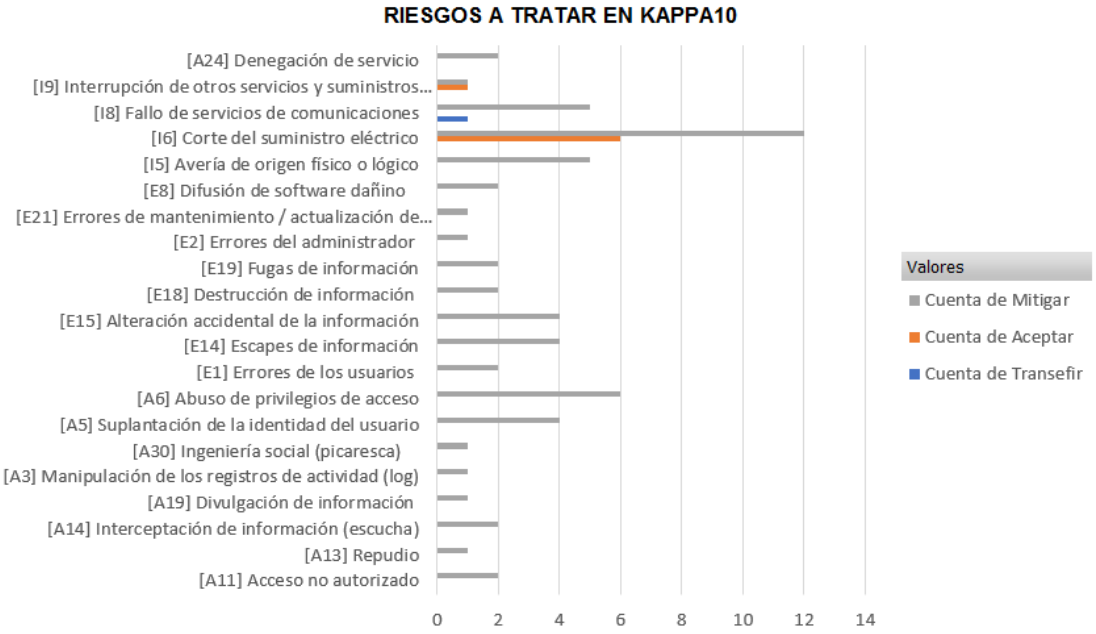
Tabla 17. (Continuación)

| Activo | Amenaza MAGERIT | Plan de tratamiento de riesgos | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | Transferir | Aceptar | Mitigar | Nomenclatura del control | Control | Descripción del control | Descripción de aplicación del control |
| [SW_PRTG] | [A19] Divulgación de información | | | X | A13.2.4 | Acuerdos de confidencialidad o de no divulgación | Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información. | La empresa tiene implementados acuerdos de confidencialidad y no divulgación que están implícitos en los contratos de los empleados. |
| [SERVICE_INTERNET_OF503] | [I6] Corte del suministro eléctrico | | | X | A11.2.2 | Servicios de suministro | Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro. | El dispositivo donde está alojado el servicio se conectará a la UPS PRO1500 para evitar fallas en su sistema. |
| [SERVICE_INTERNET_OF211] | [I6] Corte del suministro eléctrico | | | X | A11.2.2 | Servicios de suministro | Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro. | El dispositivo donde está alojado el servicio se encuentra conectado a la UPS GALLEON para evitar fallas en su sistema. |
| [SERVICE_TELEPHONE] | [I6] Corte del suministro eléctrico | | X | | | | | Se decide aceptar el riesgo por parte de la compañía por el momento, ya que se está enfocando a los empleados y al SGSI, a la mitigación de los riesgos más críticos para el negocio y para la consecución de la certificación ISO 27001:2013. |

Con ayuda de la tabla 17 fue posible identificar los riesgos críticos que más ocurren en Kappa10 Ltda. Además se pudo ver cómo están distribuidos de acuerdo con su ocurrencia, cuáles deben ser mitigados, aceptados o transferidos y cual es el nivel

de urgencia de atención de cada uno de ellos con respecto a estos valores. Lo mencionado se refleja en la siguiente figura:

Figura 4. Gráfica de la tabla 17.




Fuente: Juan Carlos Briceño.

Por ejemplo, en la figura 4 es claro que el riesgo de mayor ocurrencia es el corte del suministro eléctrico, y en el análisis de riesgos, se menciona que la forma de mitigar estos riesgos es mediante los sistemas de alimentación ininterrumpidos (UPS) que se encuentran en los racks de las oficinas 503 y 211. La importancia de esta tabla radica principalmente en su facilidad de mostrar los planes de acción que se sugieren en las recomendaciones para la mitigación de riesgos en la empresa.

# 7 RESULTADOS

El análisis de riesgos de la empresa Kappa10 Ltda. que se encuentra en este mismo documento (pág. 60 Numeral 6.2), se hacía necesario en un principio para poder aspirar a obtener la certificación ISO 27001:2013, pero durante el proceso también se generaron bases de conocimiento que no solamente van a ayudar a obtener dicha certificación, sino también contribuirán al orden y al crecimiento de la empresa. Los siguientes resultados muestran la confirmación de la aseveración realizada.

Se creó un listado de los activos de infraestructura tecnológica de la empresa hasta el momento inexistente, brindando un punto de partida para el análisis y los planes de certificación y mejora continua de la empresa. En total se identificaron 29 activos de infraestructura tecnológica.

Se inspeccionaron y documentaron los riesgos de cada uno de los 29 activos de infraestructura tecnológica de Kappa10, dando un total de 291 riesgos, 10 en promedio por cada activo. Además se documentaron las salvaguardas de cada riesgo, dando una clasificación de estos de acuerdo con su criticidad residual en 31 críticos, 11 Importantes, 68 apreciables, 111 bajos y 70 despreciables. Finalmente, la matriz orquestada para el análisis de los riesgos de seguridad de la información arrojó como resultado 70 riesgos aceptables, 152 riesgos moderados y 69 riesgos inaceptables, para un total de 291 riesgos.

Se propuso un plan de tratamiento para todos los 69 riesgos de nivel inaceptable detectados durante el análisis de riesgos de seguridad de la información, sobre los cuales se basan las recomendaciones realizadas a la empresa en este documento para mejorar su gestión del riesgo y enfocar sus esfuerzos a obtener la certificación ISO 27001:2013.

Se evaluó la mitigación de los riesgos de gestión de identidad de la empresa mediante la prueba piloto de autenticación, la cual fue exitosa, ya que permitió hacer

un correcto seguimiento de los eventos de ingreso, cambios y salida de las plataformas Fortinet que normalmente administra y soporta Kappa10 Ltda.

Se analizaron los riesgos de seguridad de la información de la infraestructura tecnológica de la empresa Kappa10 limitada, y se generaron las recomendaciones para alcanzar la certificación ISO 27001:2013.

# 8 CONCLUSIONES

El proyecto cumplió su objetivo de delimitación y análisis de los riesgos críticos de la compañía, y dirigió la atención a las recomendaciones de las posibles acciones de seguridad de la información a emprender para la empresa Kappa10, contribuyendo a la organización de servicios y procesos de esta, y a la documentación del estado actual de su infraestructura tecnológica, parte esencial de cualquier entidad.

Durante el proyecto se realizó el listado de los activos de infraestructura tecnológica, definiendo sus marcas, locaciones y características, se concretó una lista clara y concisa donde se clasificaron los elementos por su importancia para el negocio, lo que permitirá que Kappa10 pueda enfocar sus esfuerzos de mejora de una forma más estructurada y especifica.

Al inspeccionar los riesgos de cada uno de los activos de infraestructura tecnológica de una forma ordenada y dejando documentación del proceso, se facilitó a la empresa la comprensión de su estado actual en cuanto a seguridad de la información, y se creó una mayor conciencia del estado físico y lógico en el que están los activos de información de esta, lo que permitirá a las directivas la toma de decisiones acertadas de mitigación de riesgos en un futuro cercano.

Con los riesgos debidamente clasificados por su nivel de criticidad gracias a las diferentes fases del análisis basado en la metodología MAGERIT y las normas ISO 27001 y 27002, se hacen varias recomendaciones a la empresa en el plan de tratamiento de riesgos, enfocando los esfuerzos a atender los niveles inaceptables de riesgo como primera medida, lo cual permitirá a las directivas enfocar sus esfuerzos de manera sistemática a mejorar las zonas más débiles de la empresa y así llenar los requisitos para la obtención de la certificación ISO 27001:2013 en un futuro cercano.

Al haber desarrollado el proyecto aplicando la metodología de análisis de riesgos MAGERIT y usando una matriz de riesgos automatizada, se deja una

documentación completa que permite a la empresa ir mejorando por campos reales y medibles en el tiempo. Con las falencias de seguridad claras, es mucho más fácil para la empresa redirigir sus esfuerzos a los puntos de criticidad más altos, y así mitigar uno a uno los riesgos encontrados durante el proceso de análisis.

La prueba piloto de gestión de identidad fue exitosa, y ayudó a evaluar la herramienta utilizada, FortiAuthenticator, y su funcionamiento en el entorno empresarial que maneja Kappa10. De esta forma se brinda a los directivos una primera opción de mitigación del riesgo de no contar con una gestión de identidad adecuada, lo que facilitará en gran medida la toma de decisiones a este respecto.

El proyecto en general cumplió con el objetivo propuesto inicialmente, ya que se inventariaron los activos de infraestructura tecnológica de la de la empresa Kappa10 limitada, se realizó un estudio a cabalidad de cada uno de estos para identificar sus riesgos, se analizaron los riesgos de seguridad de la información encontrados y se generaron las recomendaciones que en un futuro cercano permitan a la empresa postularse para obtener la certificación ISO 27001:2013.

Este proyecto se planteó con fines educativos y de cumplimiento de objetivos de la empresa participante, a saber Kappa10 Ltda., por lo que de acuerdo con su alcance, se ha venido socializando con las partes interesadas, y se seguirá compartiendo este conocimiento dentro de la compañía para que el personal directivo y operativo se encuentre alineado con las metas trazadas por la empresa.

# 9 RECOMENDACIONES

Una vez concluido el análisis de riesgos en Kappa 10 Ltda. se hace imperativo exponer las recomendaciones a los grupos de interés del proyecto, por lo que de acuerdo con el plan de tratamiento de riesgos propuesto, se hacen las recomendaciones expuestas a continuación:

Implementar el sistema de gestión de identidad propuesto en el anexo B, el cual involucra al controlador de dominio y al dispositivo virtual FortiAuthenticator, ya que este método de gestión de identidad y control de cambios fue probado exitoso en el laboratorio de Kappa10 (Ver Anexo B). De esta forma la empresa cumplirá el requisito expresado explícitamente en el numeral A. 11 CONTROL DE ACCESO de la norma ISO 27001[66].

Los administradores de las plataformas de seguridad e infraestructura tecnológica de Kappa10 Ltda. deben otorgar los privilegios de uso de estas de acuerdo con cada rol, basándose en las labores que realice cada empleado, y apoyándose en la nueva infraestructura de gestión de identidad propuesta en el anexo B de este proyecto. En el caso de acceso a la administración de los equipos de seguridad, solamente deben tener acceso de lecto-escritura los ingenieros del área de operaciones, basándose en nombre de directorio activo.

El sistema de gestión de identidad debe contar con una política de contraseña segura, en la cual se proponga un mínimo de longitud, y el uso obligatorio de caracteres alfanuméricos, para lo cual se recomienda la activación y configuración de esta característica de FortiAuthenticator, que es una plataforma enfocada al control especifico de la autenticación de usuarios y por medio de la cual se puede implementar esta propuesta de mejora.

Se debe gestionar la capacidad de los dispositivos informáticos y de seguridad mediante el monitoreo de la herramienta PRTG (En proceso de implementación).

[66] ICONTEC. Op. Cit., p. 26.

De esta forma se verá una reacción proactiva a las posibles fallas, evitando consecuencias como la afectación del servicio.

El área de infraestructura debe continuar realizando el respaldo mensual de la configuración de los equipos Fortinet administrados y soportados por el área operativa de Kappa10, previniendo así eventos de pérdida de información y fallas de servicio prolongadas. Estas copias deben mantenerse en un repositorio seguro y redundante, como se hace ahora con Google Drive empresarial.

Se recomienda informar vía correo electrónico todo cambio que implique un corte de servicios dentro de la empresa. Además este tipo de actividades deben estar previamente aprobadas por las directivas de acuerdo con lo definido en el documento “Ventanas de mantenimiento” que se encuentra en el repositorio empresarial de Google Drive.

Es mandatorio mantener el proceso de respaldo de información semanal del servidor de controlador de dominio, y procurar seguir resguardando esta información crítica de forma segura, teniendo en cuenta que muchos de los servicios de la compañía dependen de su buen funcionamiento.

Se deben dictar capacitaciones de seguridad de la información y uso responsable de esta al interior de la empresa con una periodicidad mínima de 6 meses, con el fin de crear conciencia en los colaboradores y generar un mejor uso de los elementos brindados por la compañía.

Durante el análisis se detectó la necesidad realizar una réplica de los servicios más importantes del negocio en la nube, lo anterior con el fin de mantener siempre estable la operación. Puntualmente los servicios que se recomiendan respaldar son el directorio activo, el FortiAuthenticator, y el software de datos iTop. Esto entrará en el plan de recuperación ante desastres (DRP), que se encuentra en implementación. Las nubes de virtualización sugeridas son Amazon y Azure, por sus características de compatibilidad.

Conectar los activos de infraestructura tecnológica críticos de la empresa, como Módems, Firewalls, y servidores, a los sistemas de alimentación eléctrica

ininterrumpida (UPS), y asegurar que la autonomía de estas sea suficiente para mantener la operación hasta 4 horas de continuo, teniendo en cuenta que en la localidad de Chapinero donde se encuentra la empresa no ocurren cortes de energía más largos que este tiempo. Para este punto se recomienda la revisión de un especialista en sistemas de este tipo a las dos UPS de Kappa10.

Es imperativo que los equipos de seguridad informática marca Fortinet se mantengan actualizados en la última versión estable para evitar riesgos atados a vulnerabilidades conocidas y parchadas por el fabricante. Este proceso debe ser cíclico, y debe ser revisado como mínimo 3 veces en el año.

El área de recursos humanos debe mantener y mejorar el proceso que asegura que se firmen los acuerdos de confidencialidad y no divulgación de información importante y privada de la empresa en el momento de la contratación y en el periodo posterior a la relación laboral con Kappa10 Ltda.

Según el análisis realizado se sugiere revisar la seguridad de las redes inalámbricas en las dos oficinas de Kappa10, para asegurar que las redes inalámbricas se encuentren ocultas, tengan una clave alfanumérica de longitud considerable, y que el poder de irradiación de los puntos de acceso sea solamente el necesario para cubrir la zona de la oficina.

Asegurar que las plataformas de infraestructura tecnológica de la empresa guarden al menos 3 meses de registros para seguimiento de eventos y cambios, con lo cual se podrá realizar de forma acertada el control de cambios para cumplimiento de las normas ISO 27001:2013.

Se requiere que se mantengan parchados y actualizados los servidores de aplicativos y directorio activo de la empresa, tanto sus sistemas operativos como sus diferentes aplicaciones. Además estos deben contar con sus funciones de seguridad activas y bien configuradas para evitar cualquier tipo de robo de información o fraude informático.

Se recomienda revisar los riesgos aceptados que tienen que ver con el corte de suministros de comunicación y energía eléctrica, e incluir una forma de mitigación

dentro del DRP que se viene implementando en la empresa, por ejemplo, se sugiere validar la posibilidad de adquisición de un canal de Internet de contingencia para los servicios más importantes de la compañía, con lo que se podría evitar la pérdida total de productividad de la empresa.

Revisar los acuerdos de disponibilidad con los proveedores de servicios de Internet, fluido eléctrico, e instalaciones, para asegurar que se estén cumpliendo todos los parámetros y porcentajes del servicio, y así se asegure que no se vea perjudicada la productividad de la empresa.

# 10 BIBLIOGRAFÍA


ALEMAN NOVOA, Helena; RODRIGUEZ BARRERA, Claudia. Metodologías Para el Análisis de Riesgos en los SGSI. [2015]. [en línea] [citado el 15 de diciembre, 2018]. Disponible en internet: http://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1874

ALOMÍA ARCE, Hernán; ESCALLÓN SANTAMARÍA, Víctor y ORTEGÓN MOSQUERA, Katherine. Metodología para realización de proyectos de grado departamento de ingeniería industrial. [2007]. [en línea] [citado el 16 de mayo, 2018]. Disponible en internet: ftp://ftp.icesi.edu.co/leonardo/PGI/Guia%20Estudiantes.pdf

BERNAL BUENO, Leonardo. Proyecto WPA2-Enterprise, Radius, LDAP [2013]. [en línea] [citado el 16 de mayo, 2018]. Disponible en internet: http://informatica.gonzalonazareno.org/proyectos/2012-13/lbb.pdf

COMBODO. iTop [en línea]. [citado el 19 de noviembre de 2018]. Disponible en Internet: https://www.combodo.com/itop

CORDERO, José y GARCÍA, Yadimyr. Análisis de riesgos y recomendaciones de seguridad de la información del hospital E.S.E. San Bartolomé de Capitanejo. Trabajo de grado Especialista en seguridad informática. Málaga. Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas, Tecnologías e Ingenierías. 2016, 82p.

DAMSA. DAMSA Soluciones integrales en capital humano. DAMSA. México (2018). [en línea]. [citado el 17 de noviembre de 2018]. Disponible en Internet: https://www.damsa.com.mx/

DIRECTOR-IT. Red de datos [en línea]. ¿Qué es un Radius? Sin fecha, Párr. 1. [Consultado: el 16 de noviembre de 2018]. Disponible en Internet: http://director-it.com/index.php/es/ssoluciones/red-de-datos/240-radius.html

FERREYRA, Adriana y DE LONGHI, Ana Lía. Metodología de la investigación. Córdoba, Argentina: Encuentro Grupo Editor [2014]. [en línea] [citado el 16 de mayo, 2018]. Disponible en internet: http://bibliotecavirtual.unad.edu.co:2051/login.aspx?direct=true&db=e000xww&AN=847674&lang=es&site=eds-live

FORTINET INC. [2018]. [en línea] [citado el 25 de octubre, 2018]. Disponible en internet: https://www.fortinet.com/

FORTINET INC. Access Management and Single Sign-On [Administración de acceso e inicio único de sesión]. [2018]. [en línea] [citado el 16 de mayo, 2018]. Disponible en internet: https://www.fortinet.com/products/identity-access-management/fortiauthenticator.html

FORTINET INC. BYOD [en línea]. The Fortinet Cookbook. (2018), p. 1. [Consultado: 10 de 11 de 2018]. Disponible en Internet: https://cookbook.fortinet.com/glossary/byod/

FORTINET INC. FortiAnalyzer Virtual Appliances [Dispositivos virtuales FortiAnalyzer]. [2018]. [en línea] [citado el 16 de mayo, 2018]. Disponible en internet: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiAnalyzer.pdf

FORTINET INC. FortiAuthenticator [2017]. [en línea] [citado el 16 de mayo, 2018]. Disponible en internet: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiAuthenticator.pdf

FORTINET INC. FortiGate Virtual Appliances [Dispositivos virtuales FortiGate] [2017]. [en línea] [citado el 16 de mayo, 2018]. Disponible en internet: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_VM.pdf

FORTINET INC. FortiGate/FortiWiFi 60D Series [2016]. [en línea] [citado el 16 de mayo, 2018]. Disponible en internet: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_FortiWiFi_60D_Series.pdf

FORTINET INC. What is IoT? [en línea]. IoT Security. (2018). [Consultado: 16 de noviembre de 2018]. Disponible en Internet: https://www.fortinet.com/resources/cyberglossary/iot-security.html

FORTINET INC. Next-Generation Firewall [Firewall de siguiente generación] [2018]. [en línea] [citado el 16 de mayo, 2018]. Disponible en internet: https://www.fortinet.com/products/next-generation-firewall.html

FORTINET INC. Secure access solution [Solución de acceso seguro] [2017]. [en línea] [citado el 16 de mayo, 2018]. Disponible en internet:

https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/SG-SAA-Enterprise-Network.pdf

GARAVITO ARENAS, Juan; PALOMARES GUTIÉRREZ, David y SANTAMARÍA ORJUELA, Jhorman. Diseño de una metodología de planeación y monitoreo de los procesos clave del Organismo Nacional de Acreditación para una proyección internacional de la acreditación. Bogotá, 2015, 270p. Trabajo de grado (Ingeniería Industrial). Pontificia Universidad Javeriana. Facultad de Ingeniería.

GARCÍA TAMAYO, Rubén. Desarrollo de una intranet con Liferay (Intranet development with Liferay) [2011]. [en línea] [citado el 16 de mayo, 2018]. Disponible en internet: https://upcommons.upc.edu/bitstream/handle/2099.1/11785/PFC_GMV_Ruben_Garcia_Tamayo.pdf

GOBIERNO DE ESPAÑA. MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libros 1. [2012]. Madrid. [en línea] [citado el 20 de octubre, 2018]. Disponible en internet: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.W9NdSTFRepo

GOBIERNO DE ESPAÑA. MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libros 2. [2012]. Madrid. [en línea] [citado el 20 de octubre, 2018]. Disponible en internet: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.W9NdSTFRepo

GOBIERNO DE ESPAÑA. MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libros 3. [2012]. Madrid. [en línea] [citado el 20 de octubre, 2018]. Disponible en internet: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.W9NdSTFRepo

GUTIÉRREZ CONEO, Jesús y PINEDA ARIAS, Juan. Análisis de riesgos de seguridad y salud por procesos basado en la norma ISO 31000:2011 para el Grupo Alcomex. Trabajo de grado Ingeniería de Producción. Bogotá. Universidad Distrital Francisco José de Caldas. Facultad de Tecnología. 2016, 57p.

ICONTEC. Norma técnica ntc-iso/iec colombiana 27001 [2006]. [en línea] [citado el 16 de mayo, 2018]. Disponible en internet: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

ICONTEC. ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES [2006]. [en línea] [citado el 10 de noviembre, 2018]. Disponible en internet: http://iso27000.es/download/ControlesISO27002-2013.pdf

ICONTEC. Norma técnica ntc-iso/iec colombiana 31000 [2006]. [en línea] [citado el 16 de mayo, 2018]. Disponible en internet: https://sitios.ces.edu.co/Documentos/NTC-ISO31000_Gestion_del_riesgo.pdf

INFOSEGUR. Objetivos de la seguridad informática. [2013]. [en línea] [citado el 16 de mayo, 2018]. Disponible en internet: https://infosegur.wordpress.com/tag/confidencialidad

IT PRENEURS Y AXELOS. Curso ITIL Foundation. ed. Release 3.3.1. [2014]. Bogotá: 2013. 457p.

JARA PÉREZ, Diana. Valoración y plan de tratamiento de riesgos de seguridad de la información para los procesos incluidos en el alcance del SGSI del cliente TGE de la empresa Assurance Controltech. Trabajo de grado Ingeniería de Sistemas. Bogotá. Universidad Distrital Francisco José de Caldas. Facultad de Ingeniería. 2017. 58p.

JAUREGUI, Macarena. Los datos estadísticos: tipos y técnicas de obtención [2016]. [en línea] [citado el 16 de mayo, 2018]. Disponible en internet: https://aprendiendoadministracion.com/los-datos-estadisticos-tipos-y-tecnicas-de-obtencion/

KEY APPLICATION ASSURANCE LEVEL TEN LTDA. Kappa 10 ltda. [2018]. [en línea] [citado el 25 de octubre, 2018]. Disponible en internet: http://www.kappa10.com/

MARTINEZ ALEGRE, Francisco. ¿Qué es el directorio activo de Microsoft? [2013]. [en línea] [citado el 16 de mayo, 2018]. Disponible en internet: http://www.martinezalegre.com/2011/03/que-es-el-directorio-activo-de-microsoft/

PEREIRA MORALES, Ana y RODRIGUEZ LUNA, Yuly. *Análisis de riesgos para una empresa de consultoría*. Bogotá, 2016, 28p. Trabajo de grado (Especialista en gerencia de riesgos y seguros). Institución Universitaria Politécnico Grancolombiano. Facultad de Ingeniería.

REPUBLICA DE COLOMBIA. LEY 1273 DE 2009. [2009]. [en línea] [citado el 15 de octubre, 2018]. Disponible en internet: http://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

REPUBLICA DE COLOMBIA. LEY 719 DE 2001. [2001]. [en línea] [citado el 15 de octubre, 2018]. Disponible en internet: http://www.secretariasenado.gov.co/senado/basedoc/ley_0719_2001.html

REPUBLICA DE COLOMBIA. LEY ESTATUTARIA 1266 DE 2008. [2008]. [en línea] [citado el 15 de octubre, 2018]. Disponible en internet: http://ticbogota.gov.co/node/137

RODRIGUEZ, Daniela. Investigación aplicada: características, definición, ejemplos [2016]. [en línea] [citado el 16 de mayo, 2018]. Disponible en internet: https://www.lifeder.com/investigacion-aplicada/

ROUSE, Margaret. Gestión de identidades, ID management. [2016]. [en línea] [citado el 16 de mayo, 2018]. Disponible en internet: https://searchdatacenter.techtarget.com/es/definicion/Gestion-de-identidades-ID-management

ROUSE, Margaret. LDAP (Lightweight Directory Access Protocol). [2007]. [en línea] [citado el 15 de diciembre, 2018]. Disponible en internet: https://searchmobilecomputing.techtarget.com/definition/LDAP

ROUSE, Margaret. RADIUS (Remote Authentication Dial-In User Service). [2007]. [en línea] [citado el 15 de diciembre, 2018]. Disponible en internet: https://searchsecurity.techtarget.com/definition/RADIUS

ROUSE, Margaret. TACACS (Terminal Access Controller Access Control System). [2007]. [en línea] [citado el 15 de diciembre, 2018]. Disponible en internet: https://searchsecurity.techtarget.com/definition/TACACS

UNAD. Matriz de Análisis de Riesgos FERZAMHER. [2018]. [en línea] [citado el 16 de mayo, 2018]. Disponible en internet: http://campus07.unad.edu.co/ecbti34/pluginfile.php/1396/mod_forum/attachment/43184/Matriz%20de%20Analisis%20de%20Riesgos%20FERZAMHER%20d.xlsx

# ANEXOS

## ANEXO A. Imágenes de la infraestructura tecnológica de kappa10 Ltda.

A continuación se mostrarán algunos de los registros fílmicos de los activos tecnológicos de Kappa 10 Ltda. obtenidos durante la inspección visual.

Figura 5. FortiWiFi 60D y Modem ISP Of. 503

Fuente: Juan Carlos Briceño

Figura 6. Rack 1 Of. 503

Fuente: Juan Carlos Briceño

Figura 7. Servidores principal y WO, Switch cisco, PBX y UPS Of. 503

Fuente: Juan Carlos Briceño

Figura 8. Impresora y teléfono IP Of. 503

Fuente: Juan Carlos Briceño

Figura 9. FortiAP PU423E Of. 503

Fuente: Juan Carlos Briceño

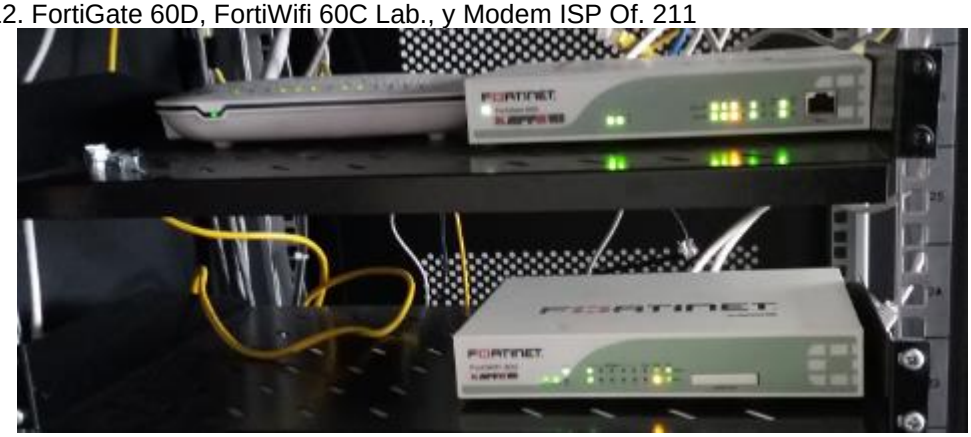
Figura 10. Cámara Of. 503

Fuente: Juan Carlos Briceño

Figura 11. Rack 1 Of. 211

Fuente: Juan Carlos Briceño

Figura 12. FortiGate 60D, FortiWifi 60C Lab., y Modem ISP Of. 211



Fuente: Juan Carlos Briceño

Figura 13. Servidor Laboratorio y UPS Of. 211

Fuente: Juan Carlos Briceño

Figura 14. Cámara Of. 211

Fuente: Juan Carlos Briceño

Figura 15. FortiAP 221B Of. 211

Fuente: Juan Carlos Briceño

**ANEXO B. Documentación técnica de la prueba piloto.**

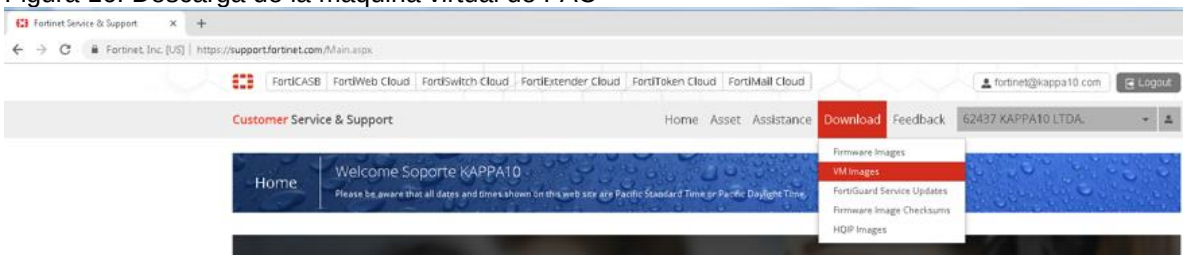
La prueba piloto se desarrollará y documentará teniendo en cuanta las recomendaciones brindadas en la documentación técnica del fabricante Fortinet. Este laboratorio comprende una de las opciones por las que puede optar la compañía Kappa10 Ltda. para mitigar el riesgo de gestión de la identidad. A continuación se listan los dispositivos que participarán en la implementación de la prueba piloto para la gestión de identidad:

- FortiAuthenticator VM (Sobre la plataforma de virtualización VMware instalada en el servidor de laboratorio de Kappa10)
- FortiWifi 60D (Oficina 503)
- FortiGate 60D (Oficina 211)
- FortiWifi 60C (Laboratorio, oficina 211)
- Directorio Activo de Windows

**Fase 1: Implementación de la máquina virtual de FortiAuthenticator.**

Las máquinas virtuales del fabricante Fortinet deben descargarse desde el sitio de Internet https://support.fortinet.com, por medio de un usuario y contraseña de cliente o partner del programa, como se puede ver en las imágenes a continuación:

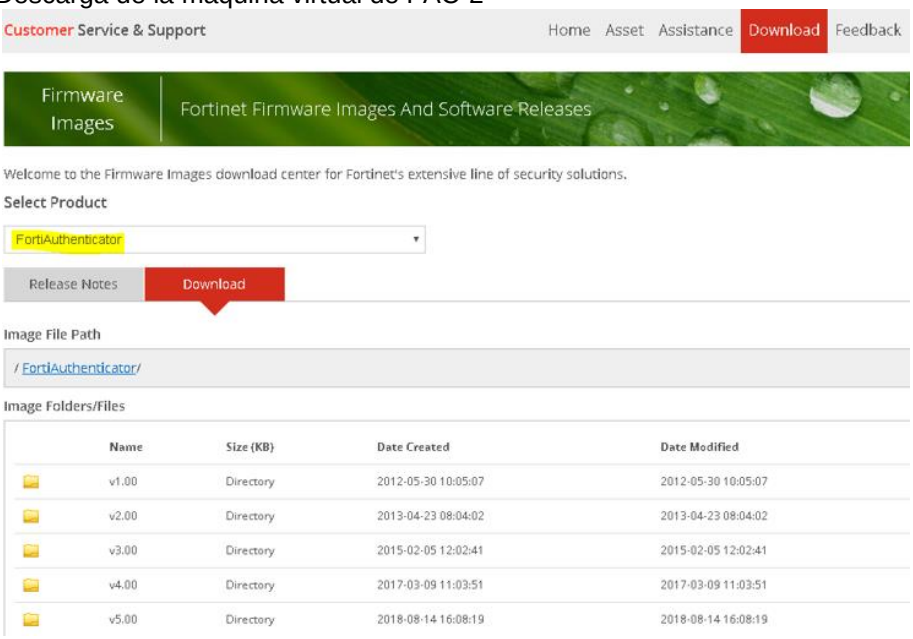
Figura 16. Descarga de la máquina virtual de FAC




Fuente: https://support.fortinet.com/Main.aspx

Se selecciona la parte de Download/VM Images, la cual redirige a la página de descarga de las máquinas virtuales que se encuentran en las mismas carpetas que las versiones de firmware de los equipos:

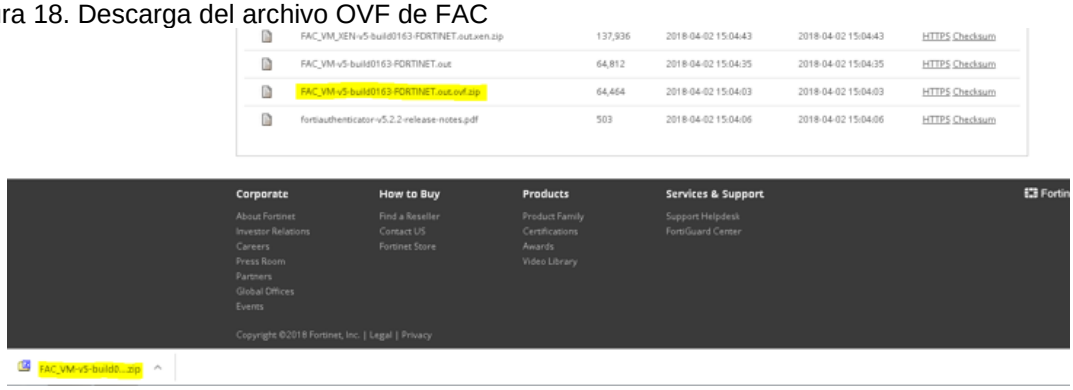
Figura 17. Descarga de la máquina virtual de FAC-2




Fuente: https://support.fortinet.com/Download/FirmwareImages.aspx

Finalmente se elige la distribución compatible con VMware y se descarga el archivo OVF de la versión de FortiAuthenticator (FAC) compatible con los dispositivos de la prueba piloto, la versión 5.2.2:

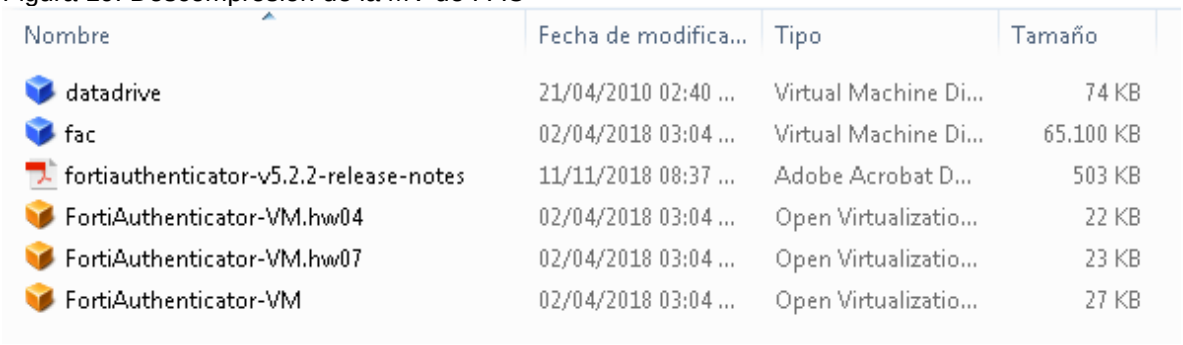
Figura 18. Descarga del archivo OVF de FAC




Fuente: https://support.fortinet.com/Download/FirmwareImages.aspx

Se descomprime la descarga, en la cual viene preconfigurada la máquina virtual del FAC lista para ser importada:

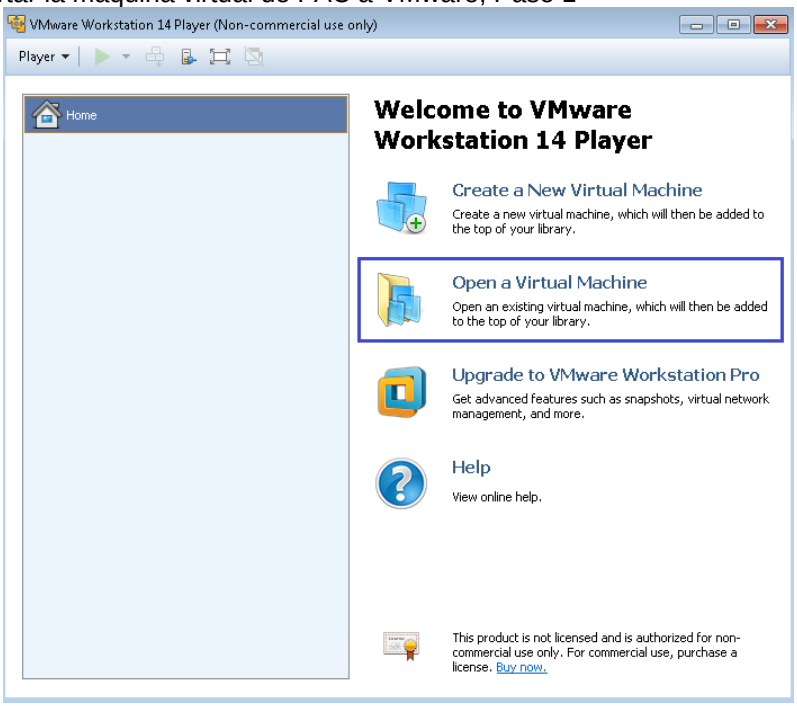
Figura 19. Descompresión de la MV de FAC




Fuente: Juan Carlos Briceño

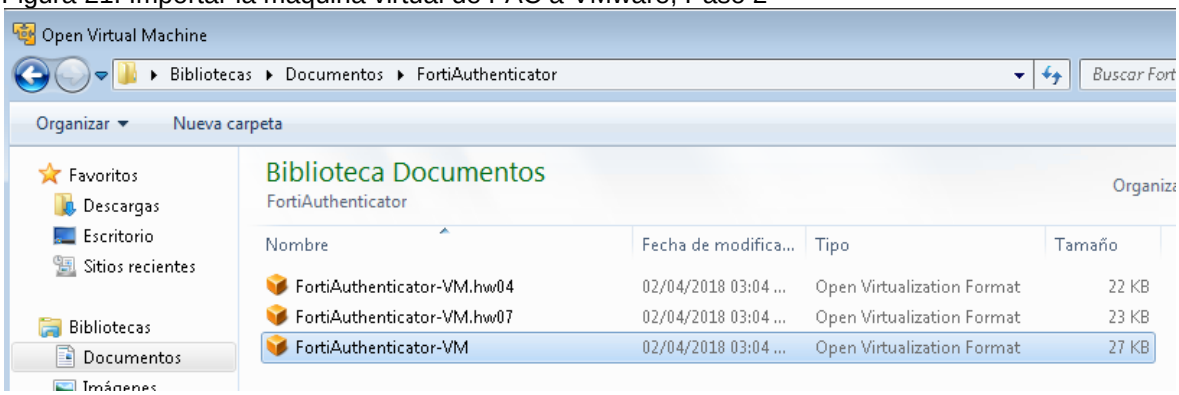
Desde VMware se selecciona la opción "*Open a virtual machine*", y se selecciona el archivo llamado "FortiAuthenticator-VM", que es el que se importará para que funcione la máquina, como se puede ver en las siguientes 3 imágenes:

Figura 20. Importar la máquina virtual de FAC a VMware, Paso 1



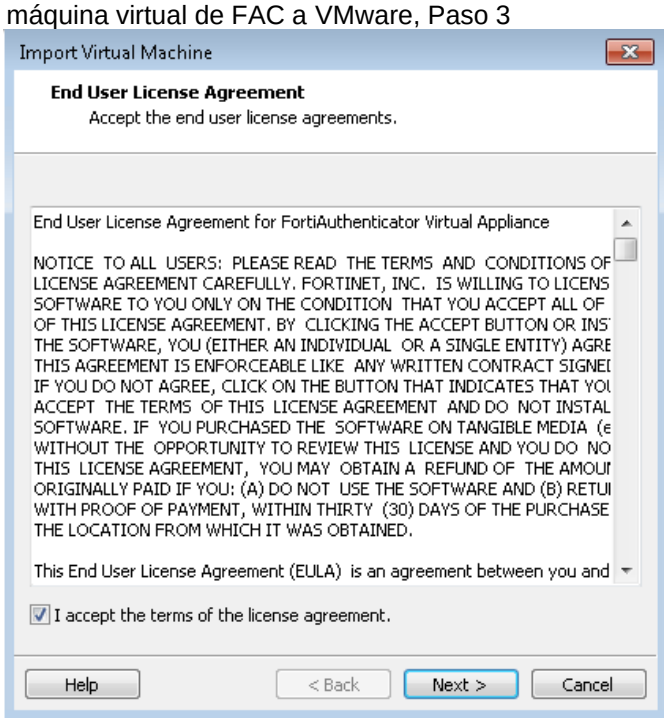

Fuente: Juan Carlos Briceño

Figura 21. Importar la máquina virtual de FAC a VMware, Paso 2




Fuente: Juan Carlos Briceño

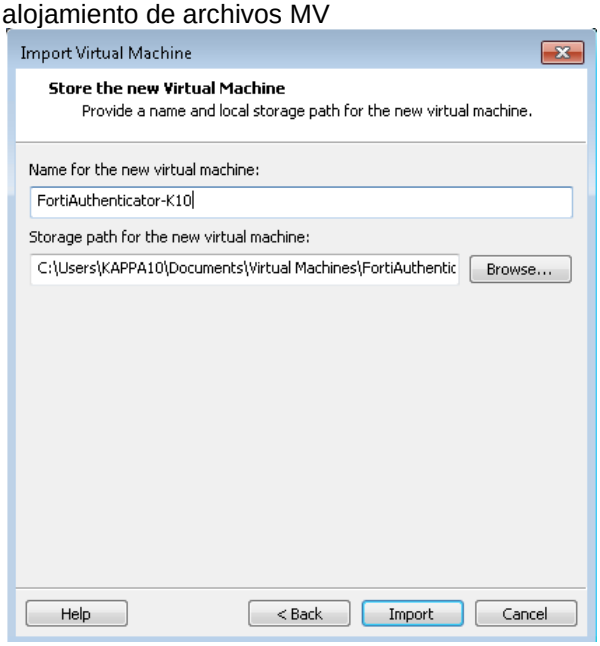
Figura 22. Importar la máquina virtual de FAC a VMware, Paso 3




Fuente: Juan Carlos Briceño

Se importa la máquina virtual y se selecciona el sitio del servidor donde se van a alojar los archivos de configuración y disco virtual:

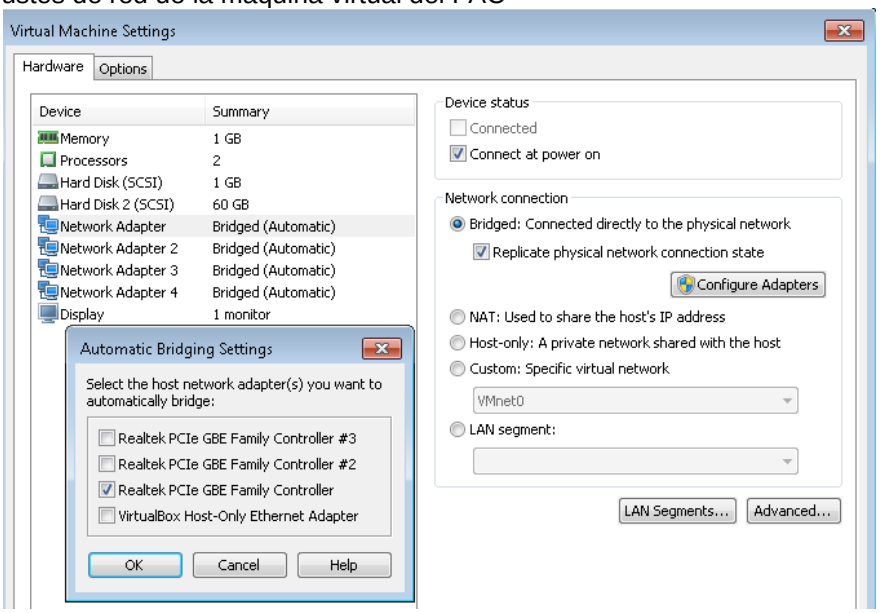
Figura 23. Definición de alojamiento de archivos MV




Fuente: Juan Carlos Briceño

La máquina virtual importada aparecerá de la siguiente manera en el VMware:

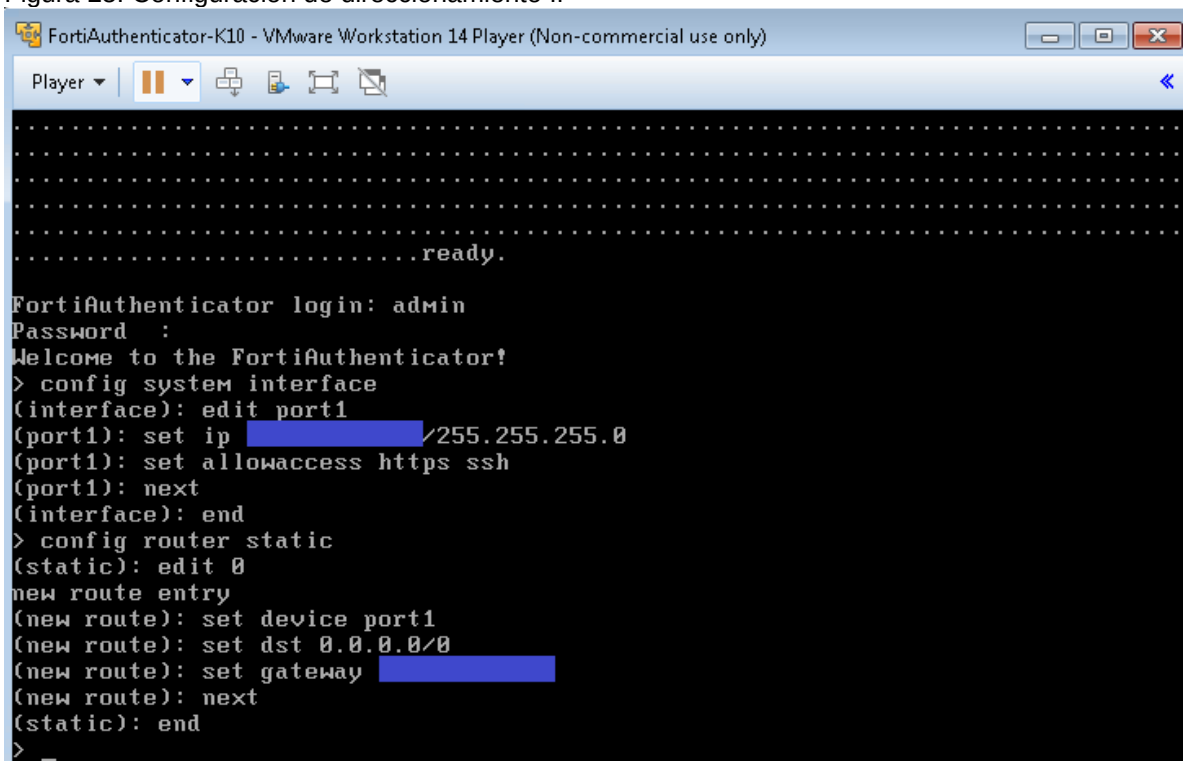
Figura 24. Ajustes de red de la máquina virtual del FAC




Fuente: Juan Carlos Briceño

Después de realizar los ajustes se enciende la máquina virtual con el botón de arranque del VMware. Por defecto tiene una licencia de prueba de 15 días, suficiente para las pruebas deseadas. Al ingresar por la consola es necesario configurar una dirección IP con su respectiva mascara de red al puerto 1 como se muestra a continuación:

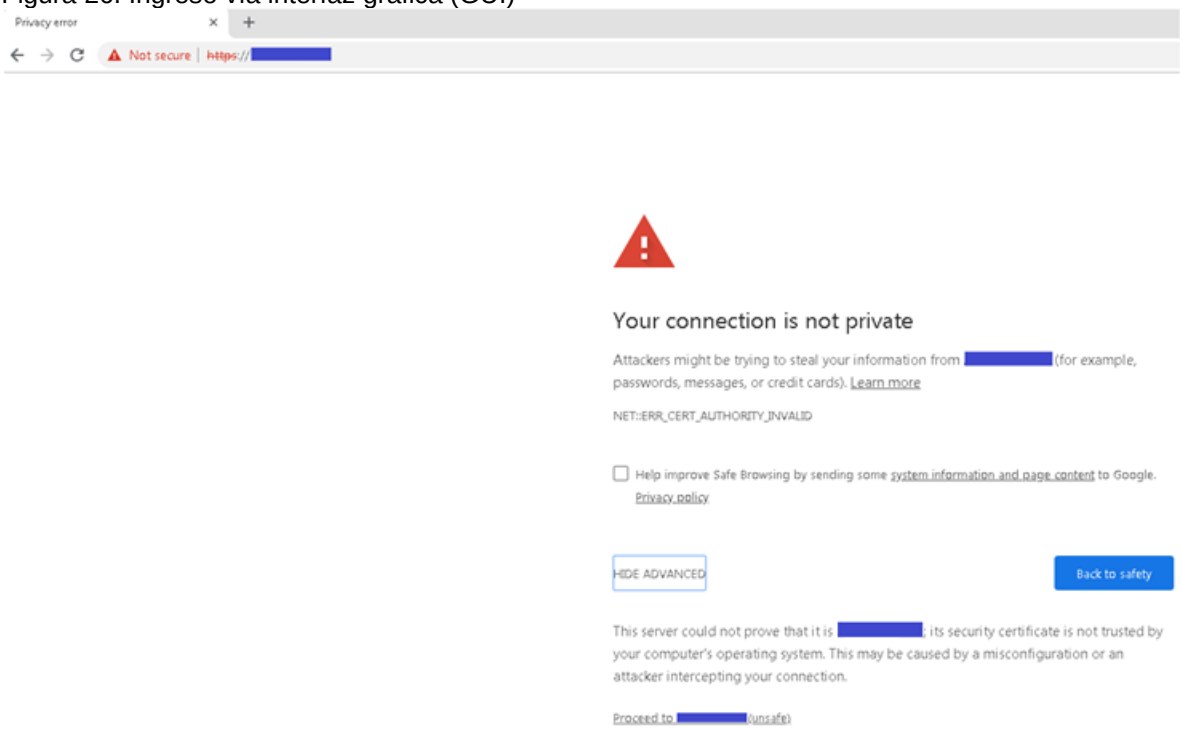
Figura 25. Configuración de direccionamiento IP




Fuente: Juan Carlos Briceño

Después de esta configuración ya es posible ingresar a administrar el nuevo FortiAuthenticator desde el navegador:

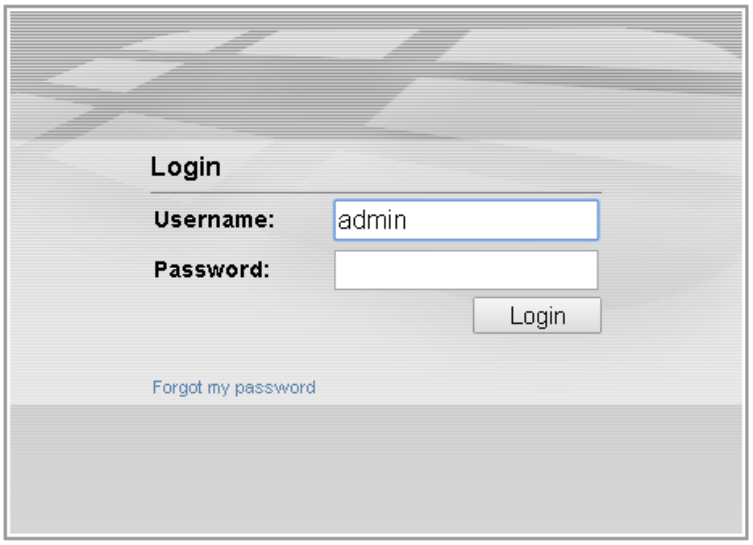
Figura 26. Ingreso vía interfaz gráfica (GUI)




Fuente: Juan Carlos Briceño

Se ingresa con el usuario por defecto, “admin”, y el espacio de contraseña en blanco (Estos parámetros deben cambiarse para evitar riesgos de seguridad en el acceso):

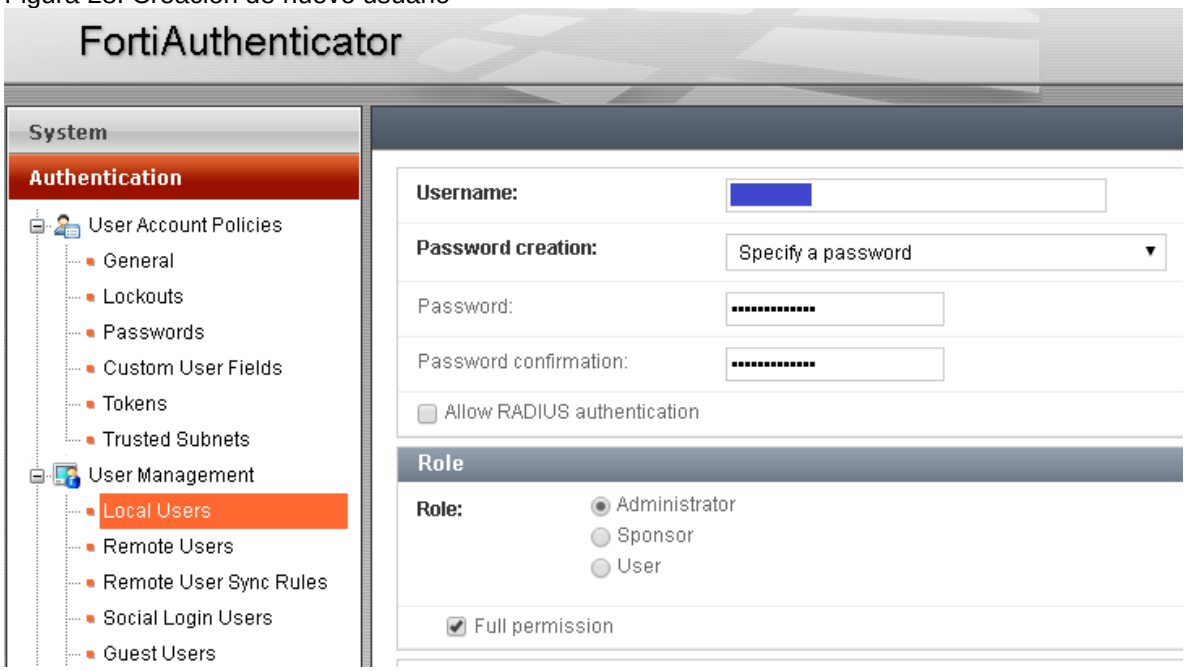
Figura 27. Ingreso por defecto al FAC




Fuente: Juan Carlos Briceño

Se crea un nuevo usuario administrador con seguridad, para poder eliminar el usuario administrador por defecto posteriormente:

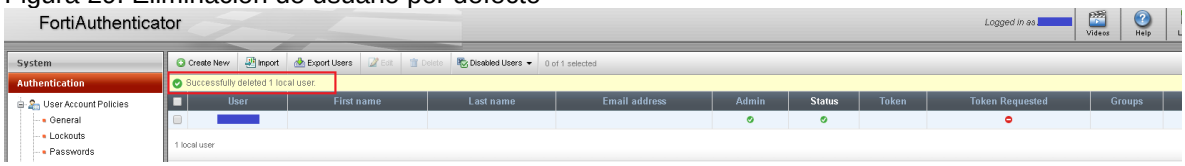
Figura 28. Creación de nuevo usuario




Fuente: Juan Carlos Briceño

Es necesario salir de la plataforma y volver a ingresar mediante el nuevo usuario que se acaba de crear, y después se realiza la eliminación del usuario “admin”:

Figura 29. Eliminación de usuario por defecto



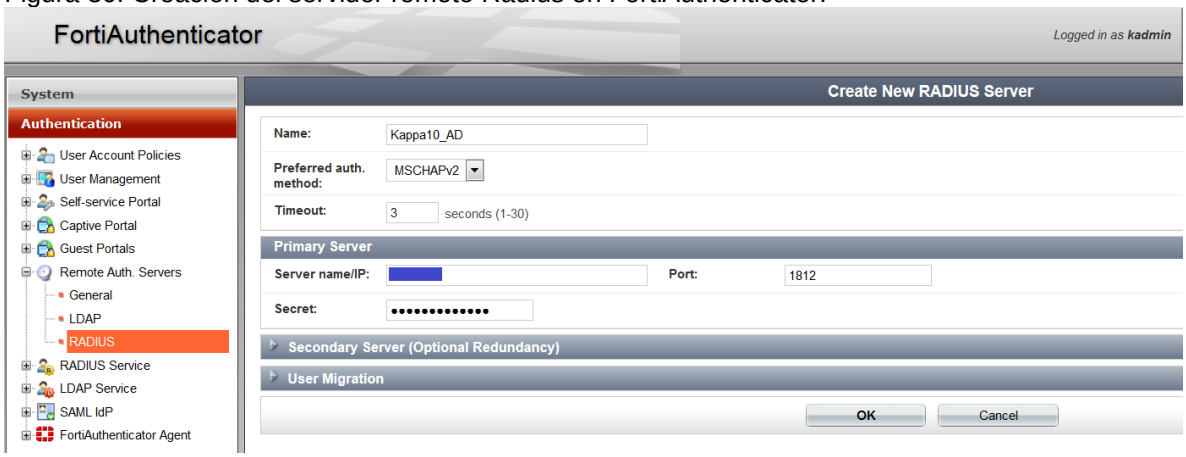

Fuente: Juan Carlos Briceño

**Fase 2: Configuración de integración del directorio activo con FortiAuthenticator.**

Para integrar el FortiAuthenticator VM con el Directorio activo es necesario que este tenga alcanzabilidad del servidor y que además tenga permisos para comunicarse con este. En este caso ambos equipos se encuentran en la misma red, por lo que no es necesario realizar nada adicional en cuestión de conectividad.

Desde el menú "Authentication > Remote Auth Servers > Radius" se procede a crear un nuevo servidor, el cual contendrá los parámetros necesarios para que el FortiAuthenticator pueda leer la información de usuarios administradores que estarán en este, usando el protocolo Radius[67].

Figura 30. Creación del servidor remoto Radius en FortiAuthenticator.

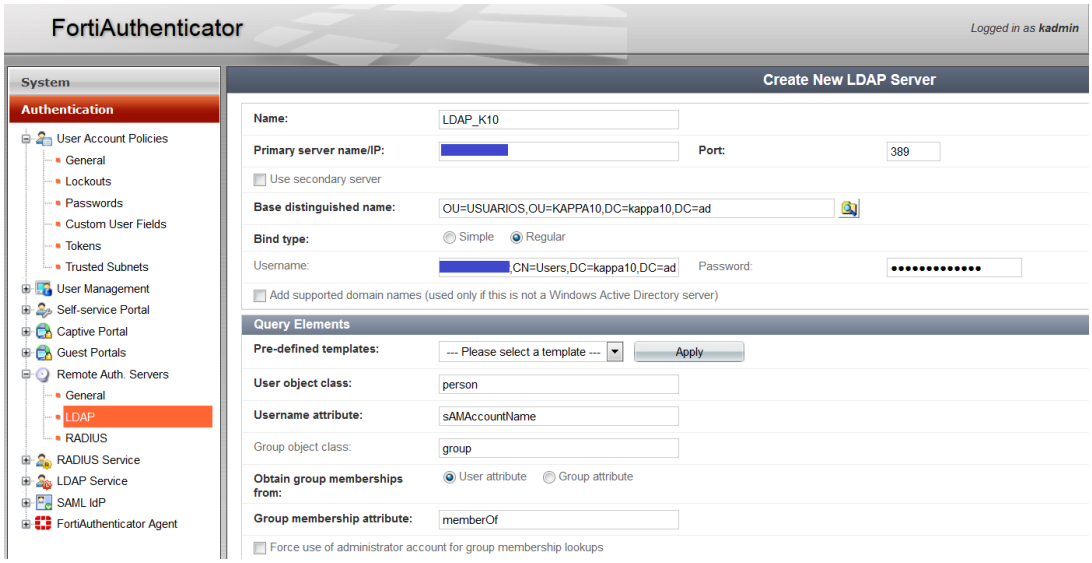



Fuente: Juan Carlos Briceño

Despues se crea un servidor tipo LDAP desde el menú "Authentication > Remote Auth Servers > LDAP", con los parámetros de lectura del directorio activo de Kappa10, como el *Base distinguished name* el usuario con el cual se leerá la información y el password de este.

[67] DIRECTOR-IT. Red de datos [en línea]. ¿Qué es un Radius? Sin fecha, Párr. 1. [Consultado: el 16 de noviembre de 2018]. Disponible en Internet: http://director-it.com/index.php/es/ssoluciones/red-de-datos/240-radius.html

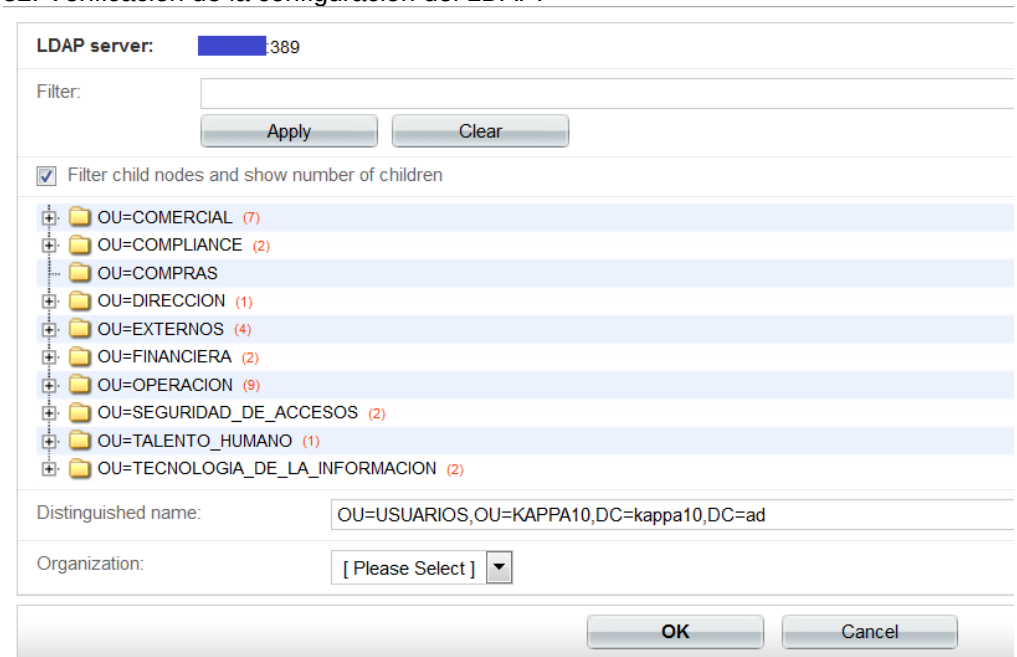
Figura 31. Creación del servidor remoto LDAP en FortiAuthenticator.




Fuente: Juan Carlos Briceño

Ahora que el directorio activo es visible desde el FortiAuthenticator, lo que se puede confirmar haciendo clic en el botón de inspección al lado del parámetro de *Base distinguished name*.

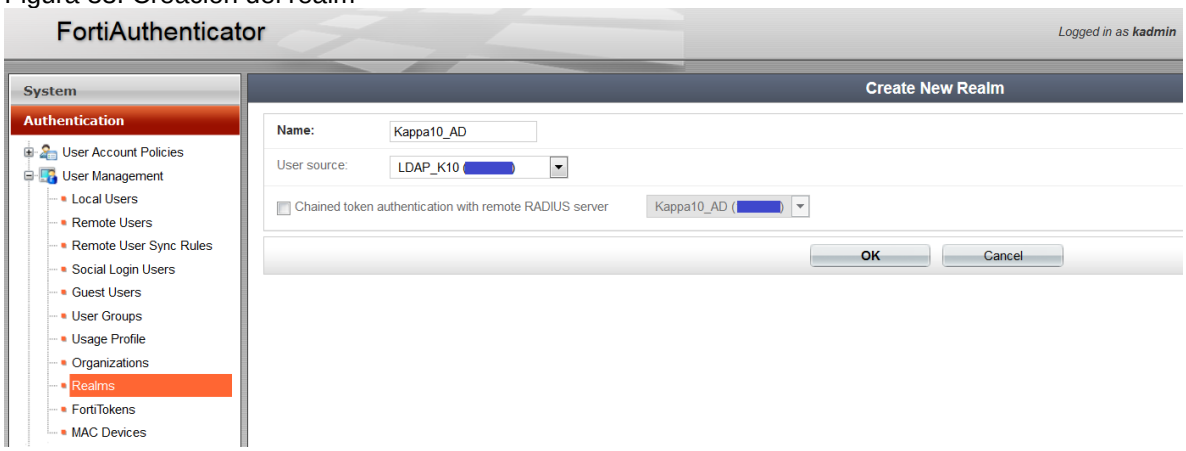
Figura 32. Verificación de la configuración del LDAP.




Fuente: Juan Carlos Briceño

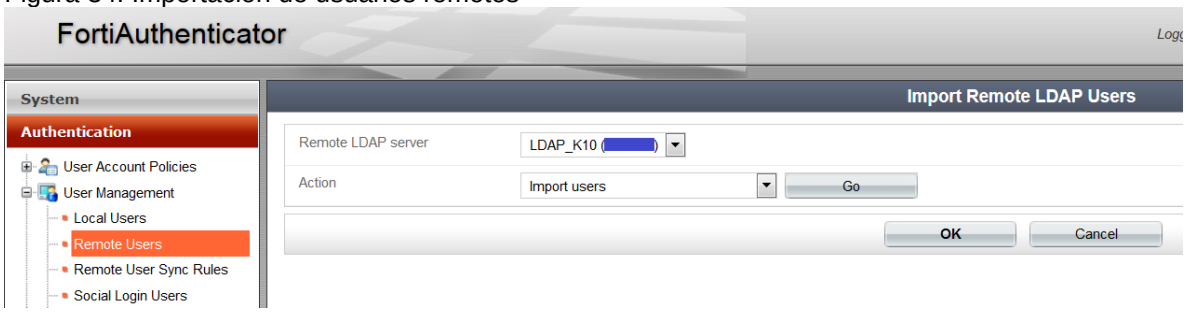
Después de concretar la conexión entre FortiAuthenticator y directorio activo es necesario crear un *realm* o campo en el menú “Authentication > User Management > Realms”. Una vez hecho esto se deben importar los usuarios que se utilizarán para la autenticación en los diferentes firewalls Fortinet utilizados en la prueba piloto. Para esto se debe ir al menú “Authentication > User Management > Remote Users”, dar clic al botón “Import”, y en la pantalla seleccionar el servidor remoto que se ha creado previamente.

Figura 33. Creación del realm




Fuente: Juan Carlos Briceño

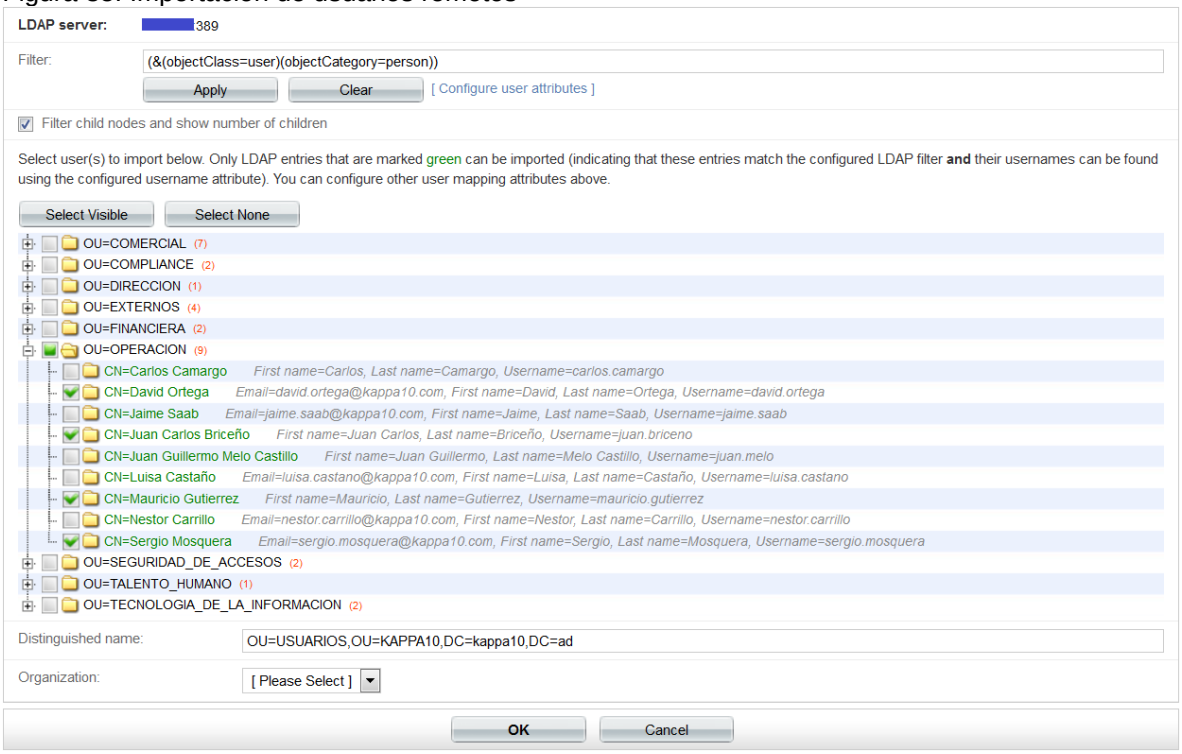
Figura 34. Importación de usuarios remotos




Fuente: Juan Carlos Briceño

Acto seguido se presiona el botón “Go”, donde mostrará una pantalla en la cual se seleccionarán los usuarios de los ingenieros que administrarán los equipos de seguridad marca Fortinet.

Figura 35. Importación de usuarios remotos



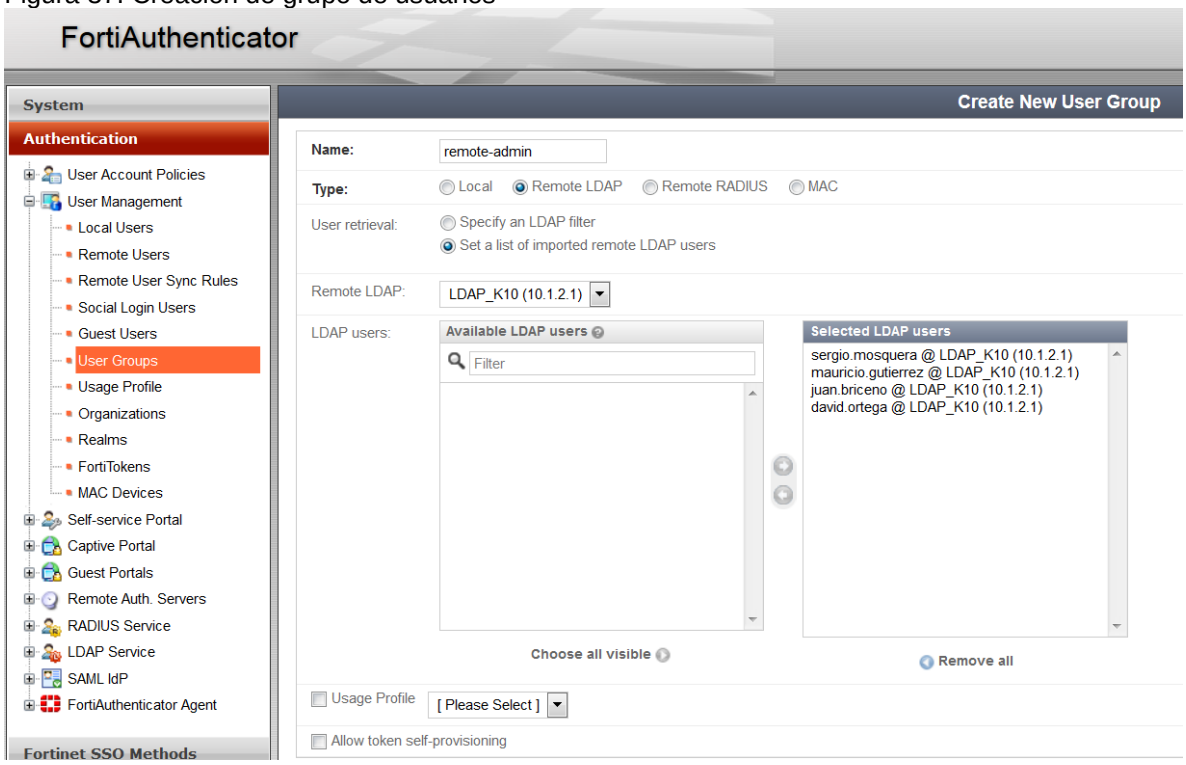

Fuente: Juan Carlos Briceño

Con los usuarios importados se procede a crear un grupo de usuarios remotos que los contenga, esto se hace desde el menú “Authentication > User Management > User Groups”.

Figura 36. Usuarios importados


Fuente: Juan Carlos Briceño

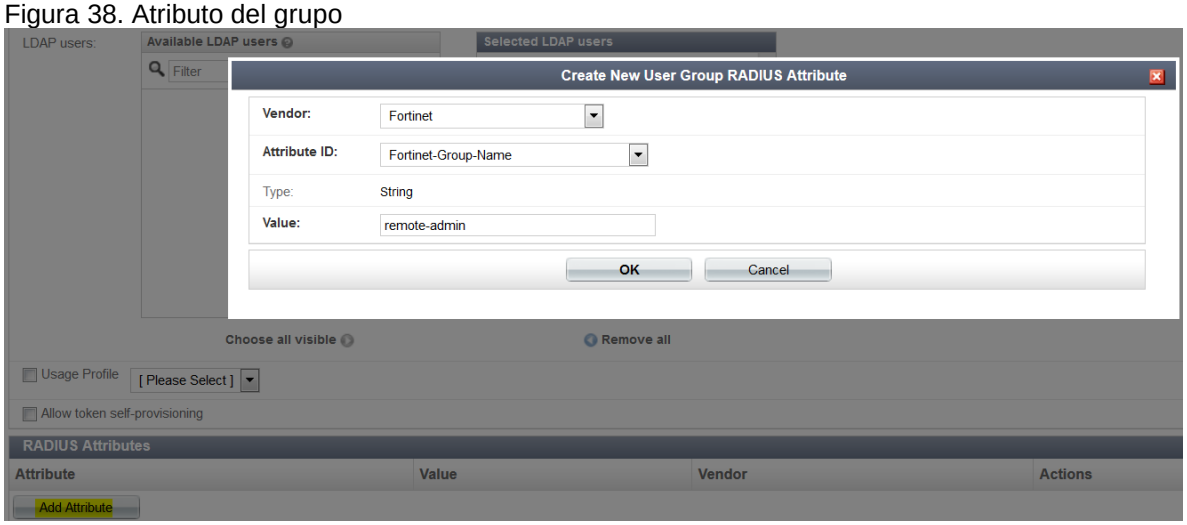
Figura 37. Creación de grupo de usuarios




Fuente: Juan Carlos Briceño

Cuando se da clic al botón OK se despliega una nueva opción, llamada "*Add Attibute*" o añadir un atributo, la cual permite crear una referencia a algo externo, en este caso un nombre de grupo del fabricante Fortinet con el valor "remote-admin", que es el nombre que se pondrá al grupo contenedor de los usuarios remotos en los Firewalls.

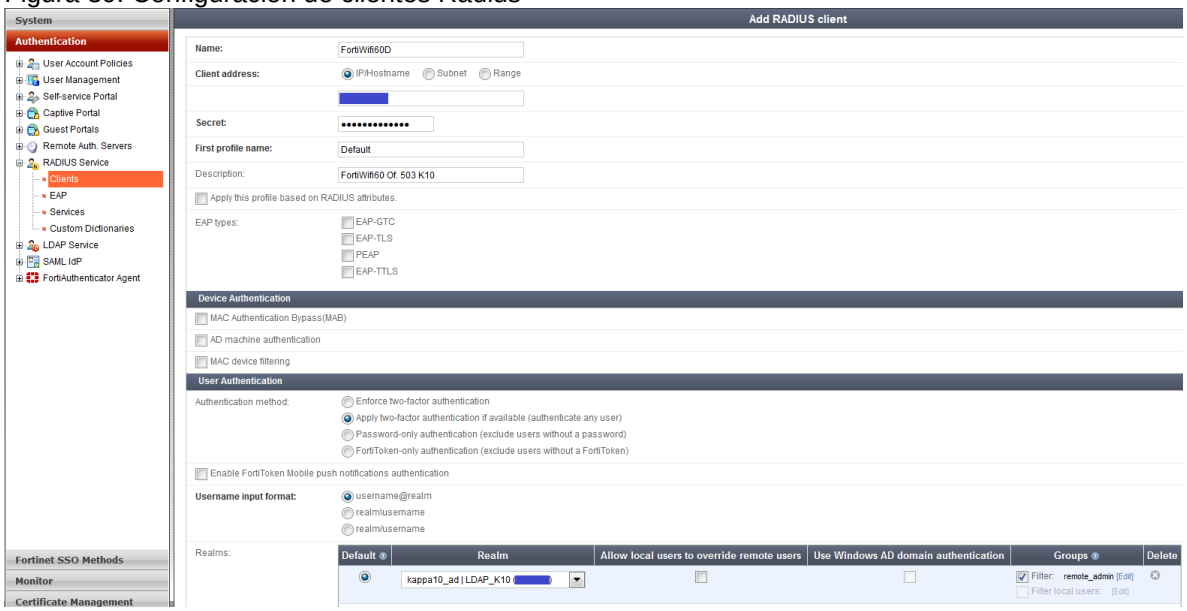
Figura 38. Atributo del grupo




Fuente: Juan Carlos Briceño

A continuación, se configuran los clientes Radius, en este caso los firewalls de las oficinas 503 y 211 de la empresa, y así se deja preparado el escenario para comenzar la configuración de gestión de identidad.

Figura 39. Configuración de clientes Radius

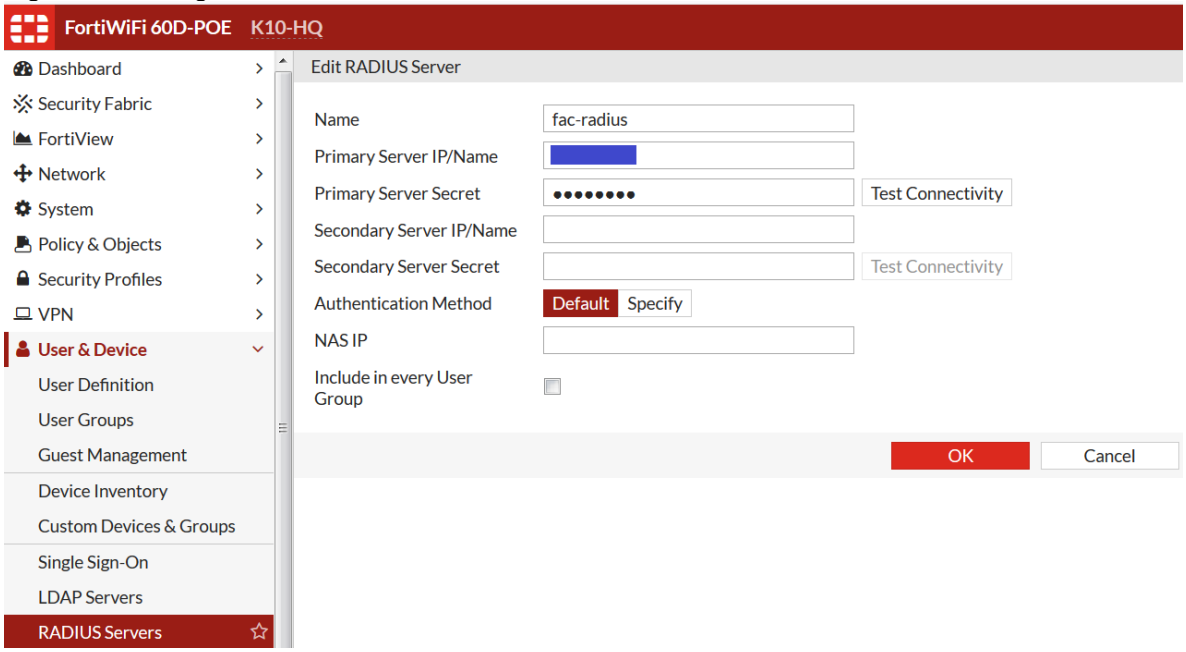



Fuente: Juan Carlos Briceño

**Fase 3. Configuración de integración de los Firewalls de siguiente generación con el FortiAuthenticator.**

Para poder administrar los Firewalls con una gestión de identidad adecuada, primero debemos crear el servidor de autenticación Radius remoto. Esto se realiza mediante el menú “User & Device > Radius Servers”, donde se pondrá un nombre al nuevo servidor (fac-radius), la dirección IP del FortiAuthenticator, y la misma clave que se configuró en el FortiAuthenticator para los clientes Radius.

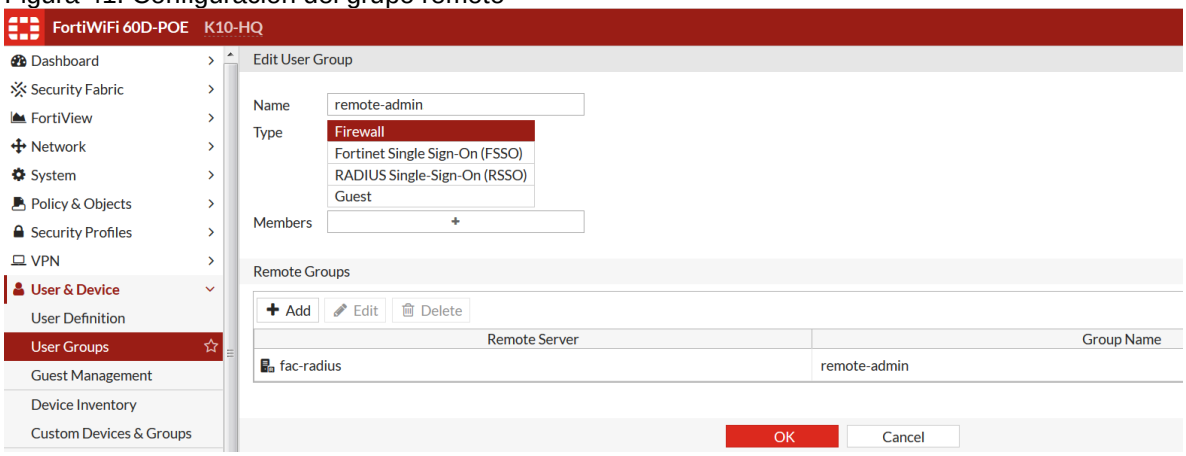
Figura 40. Configuración de servidor Radius Oficina 503




Fuente: Juan Carlos Briceño

Despues se creará un grupo que se empareje con el servidor Radius previamente configurado, con lo cual solo faltará crear el usuario remoto en el Firewall para lograr la autenticación.

Figura 41. Configuración del grupo remoto




Fuente: Juan Carlos Briceño

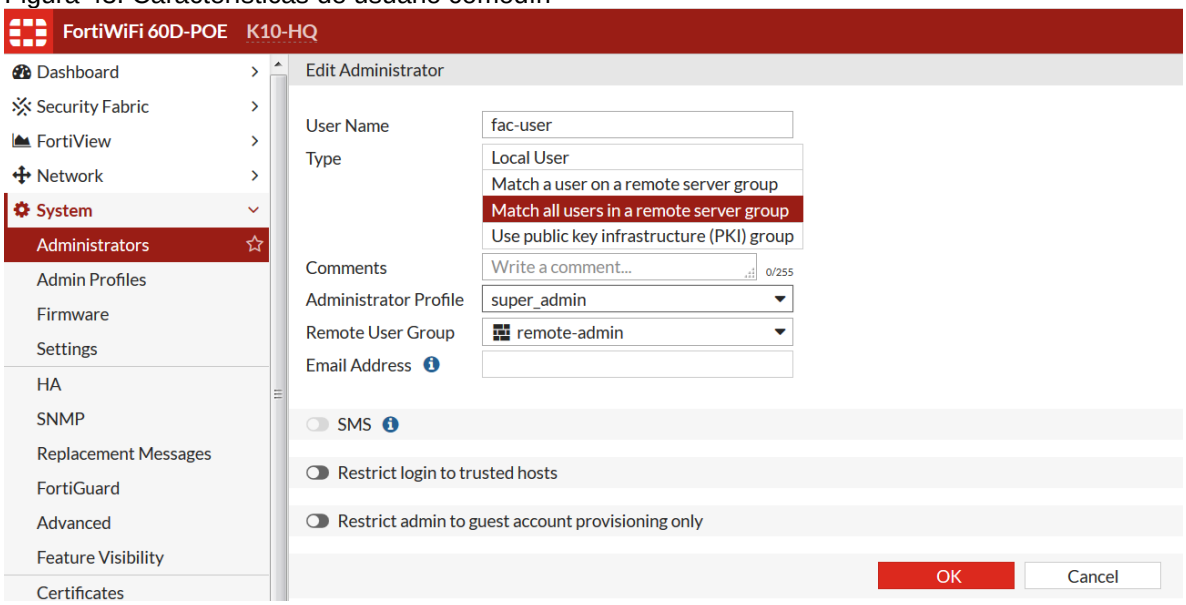
Una vez cumplidos estos pasos, es necesario configurar el usuario maestro en modo comodín, que permita al FortiAuthenticator hacer la autenticación de forma implícita con los usuarios de cada uno de los ingenieros de Kappa10. Para poder hacer esta labor, se debe ingresar con un usuario administrador de cada firewall, y crear el nuevo usuario que utilizará el FortiAuthenticator, esto se hace desde el menú “System > Administrators”.

Figura 42. Creación de nuevo usuario comodín en el firewall


Fuente: Juan Carlos Briceño

Dando clic al botón “Create New” se procede a crear el usuario de FortiAuthenticator con las características de administración que se le van a heredar a los usuarios remotos de los ingenieros de Kappa10.

Figura 43. Características de usuario comodín




Fuente: Juan Carlos Briceño

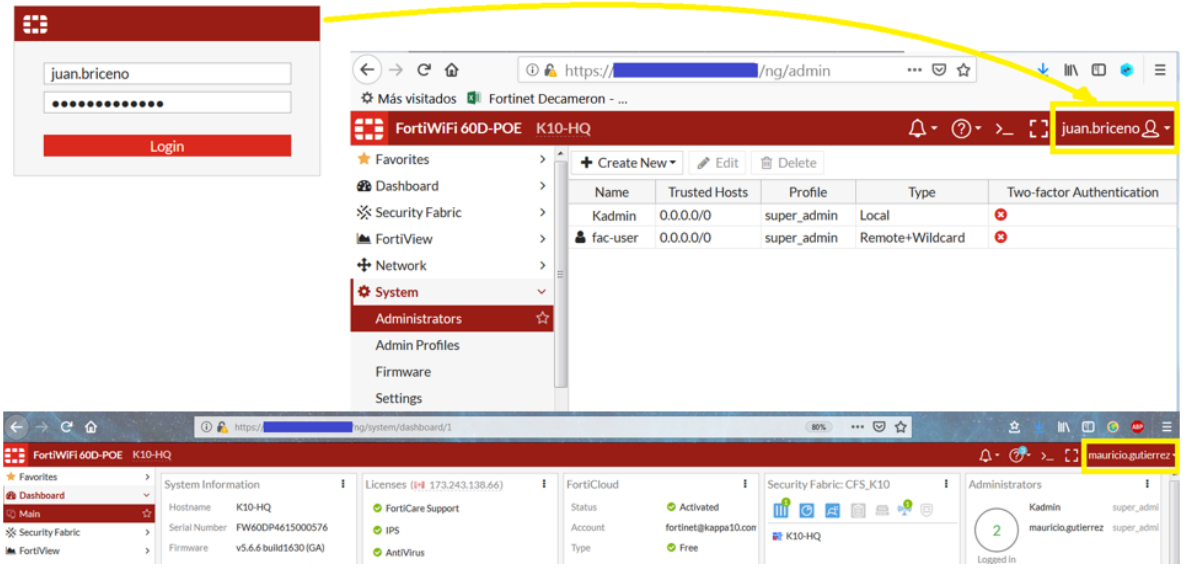
Se repiten los mismos pasos en el firewall de la oficina 211 para poder autenticar el inicio de sesión con el usuario de directorio activo por medio del protocolo Radius, y se procede a realizar las pruebas.

**Fase 4: Pruebas y resultados.**

Finalmente, es hora de realizar la prueba de inicio de sesión con el usuario de directorio activo, conservando así el usuario del directorio activo que identifica a cada uno de los ingenieros. Se realizará la prueba de autenticación en los firewalls de las dos oficinas, la cual fue exitosa de acuerdo con las siguientes imágenes y logs de prueba:

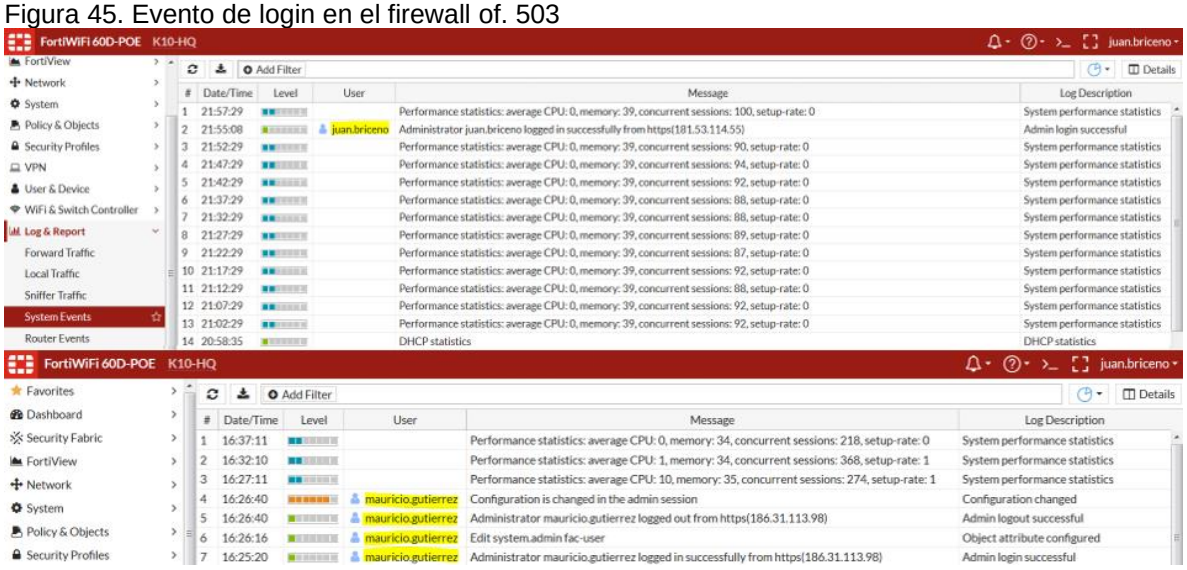
## Pruebas en el FortiWifi60D Oficina 503:

Figura 44. Ingreso al firewall de la oficina 503 con usuario remoto



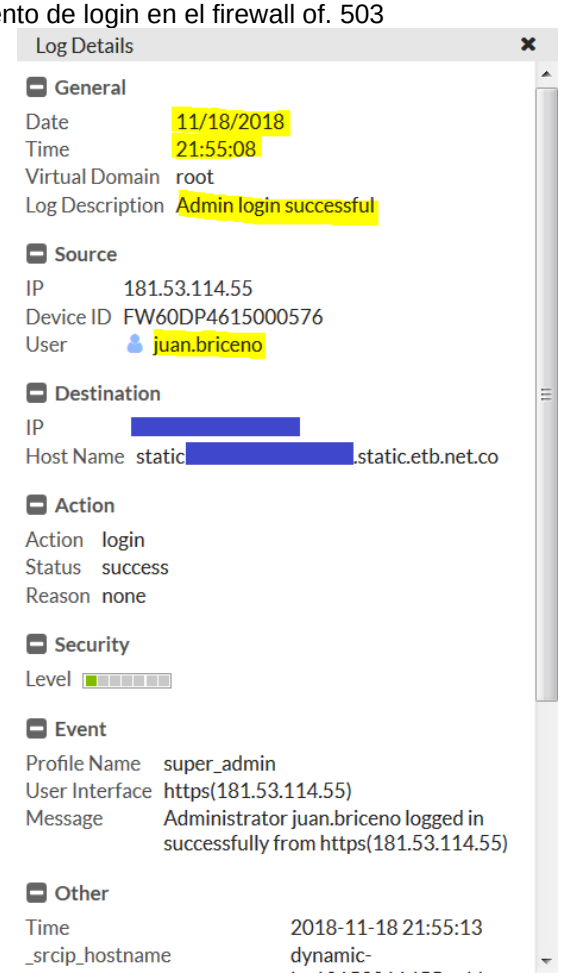

Fuente: Juan Carlos Briceño

Figura 45. Evento de login en el firewall of. 503




Fuente: Juan Carlos Briceño

Figura 46. Detalle del evento de login en el firewall of. 503



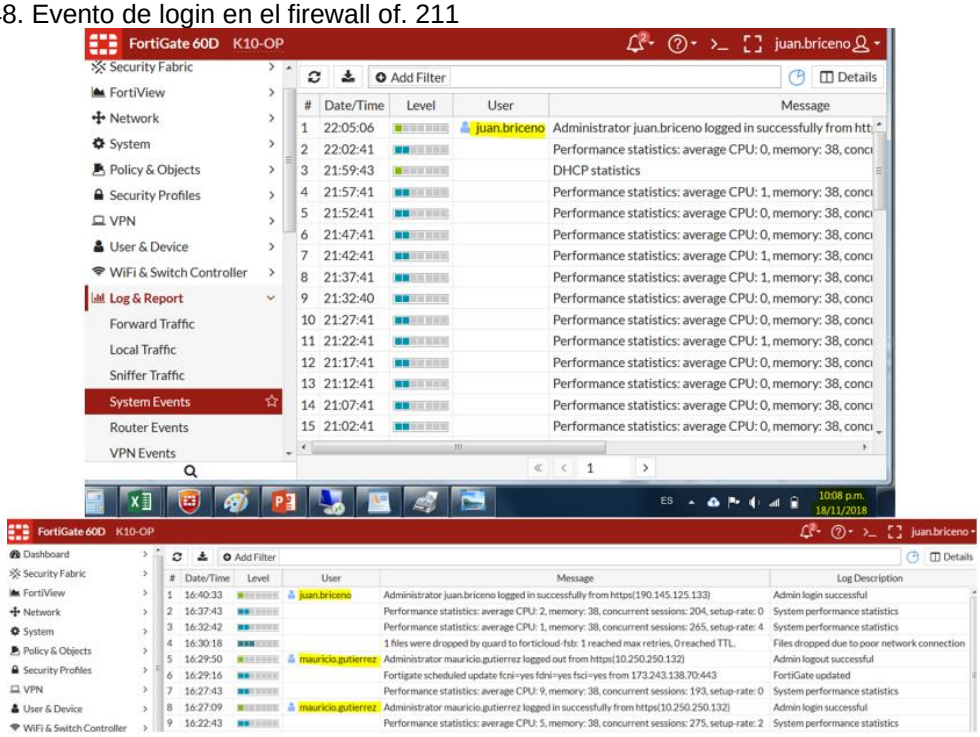

Fuente: Juan Carlos Briceño

## Pruebas en el FortiGate60D Oficina 211:

Figura 47. Ingreso al firewall de la oficina 211 con usuario remoto

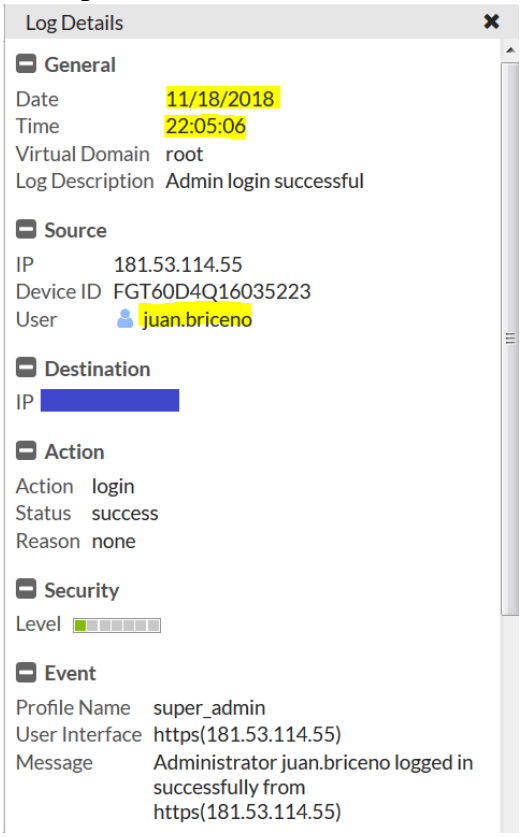

Fuente: Juan Carlos Briceño

Figura 48. Evento de login en el firewall of. 211




Fuente: Juan Carlos Briceño

Figura 49. Detalle del evento de login en el firewall of. 211

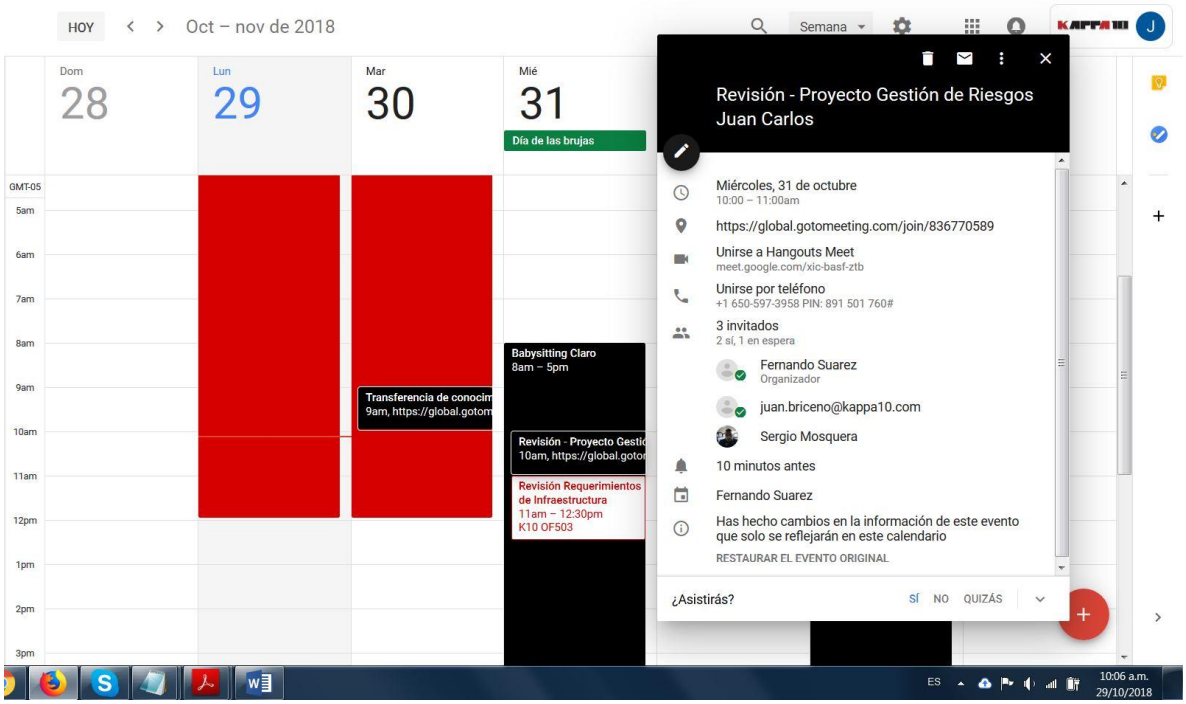



Fuente: Juan Carlos Briceño

**ANEXO C. Registros de entrevistas y reuniones Kappa10.**

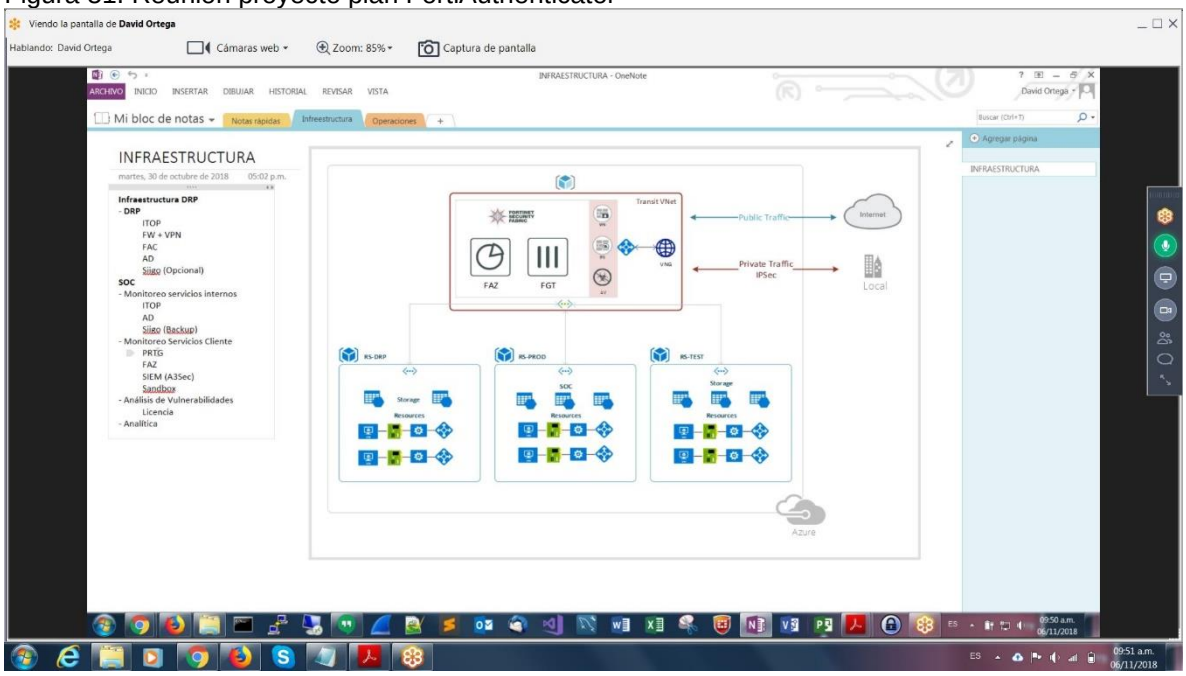
En este aparte se listan los registros de algunas de las reuniones y entrevistas sostenidas con los miembros de las áreas de operaciones y conformidad de Kappa10 Ltda. Estos registros corroboran que la información del proyecto es real y fue confirmada con la empresa blanco del análisis.

Figura 50. Programación entrevista proyecto



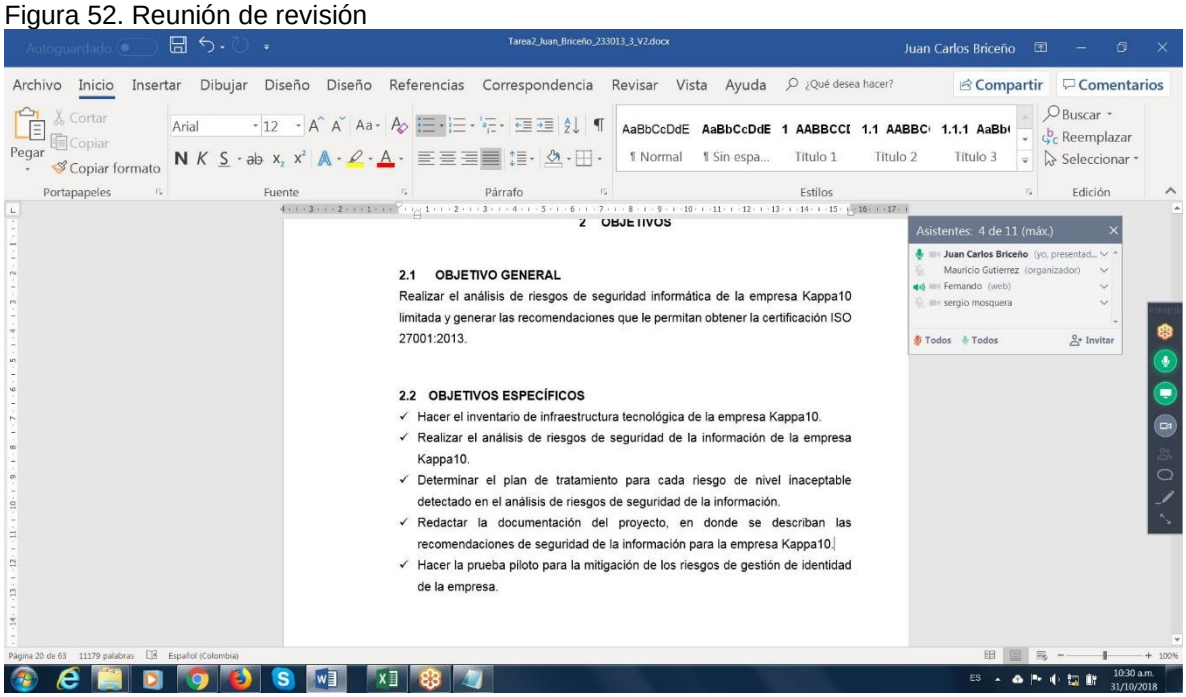

Fuente: Juan Carlos Briceño

Figura 51. Reunión proyecto plan FortiAuthenticator



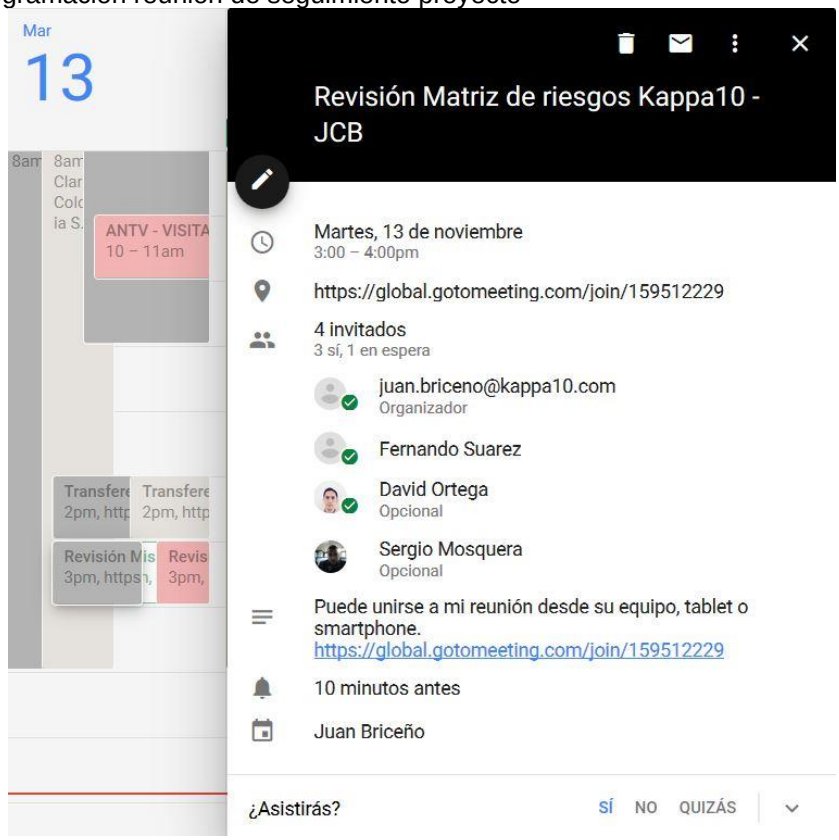

Fuente: Juan Carlos Briceño

Figura 52. Reunión de revisión




Fuente: Juan Carlos Briceño

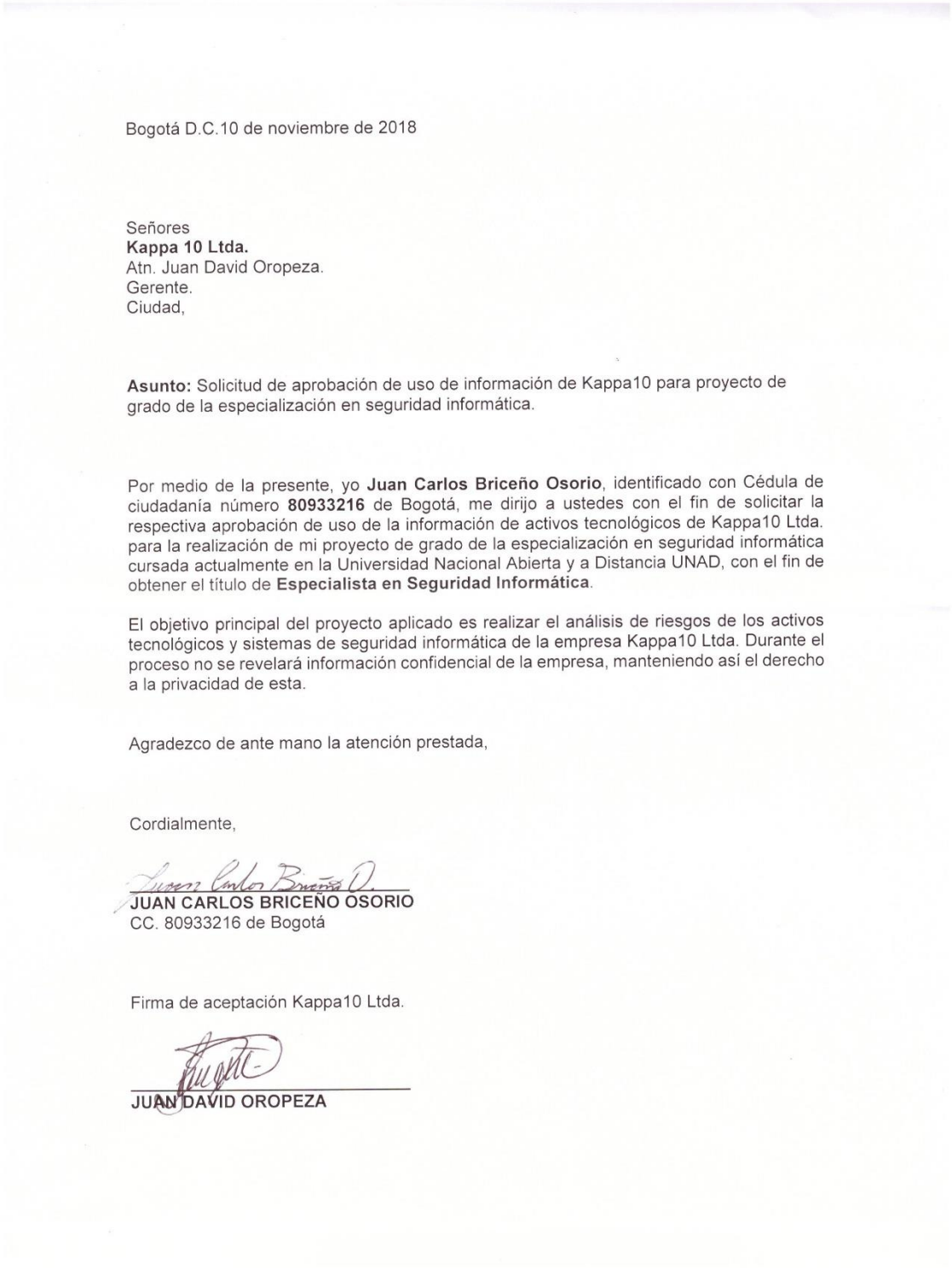
Figura 53. Programación reunión de seguimiento proyecto




Fuente: Juan Carlos Briceño

## ANEXO D. Carta de aprobación del uso de información de Kappa10.

Figura 54. Carta de solicitud de aprobación de gerencia Kappa10



Bogotá D.C.10 de noviembre de 2018

Señores
**Kappa 10 Ltda.**
Atn. Juan David Oropeza.
Gerente.
Ciudad,

**Asunto:** Solicitud de aprobación de uso de información de Kappa10 para proyecto de grado de la especialización en seguridad informática.

Por medio de la presente, yo **Juan Carlos Briceño Osorio**, identificado con Cédula de ciudadanía número **80933216** de Bogotá, me dirijo a ustedes con el fin de solicitar la respectiva aprobación de uso de la información de activos tecnológicos de Kappa10 Ltda. para la realización de mi proyecto de grado de la especialización en seguridad informática cursada actualmente en la Universidad Nacional Abierta y a Distancia UNAD, con el fin de obtener el título de **Especialista en Seguridad Informática**.

El objetivo principal del proyecto aplicado es realizar el análisis de riesgos de los activos tecnológicos y sistemas de seguridad informática de la empresa Kappa10 Ltda. Durante el proceso no se revelará información confidencial de la empresa, manteniendo así el derecho a la privacidad de esta.

Agradezco de ante mano la atención prestada,

Cordialmente,

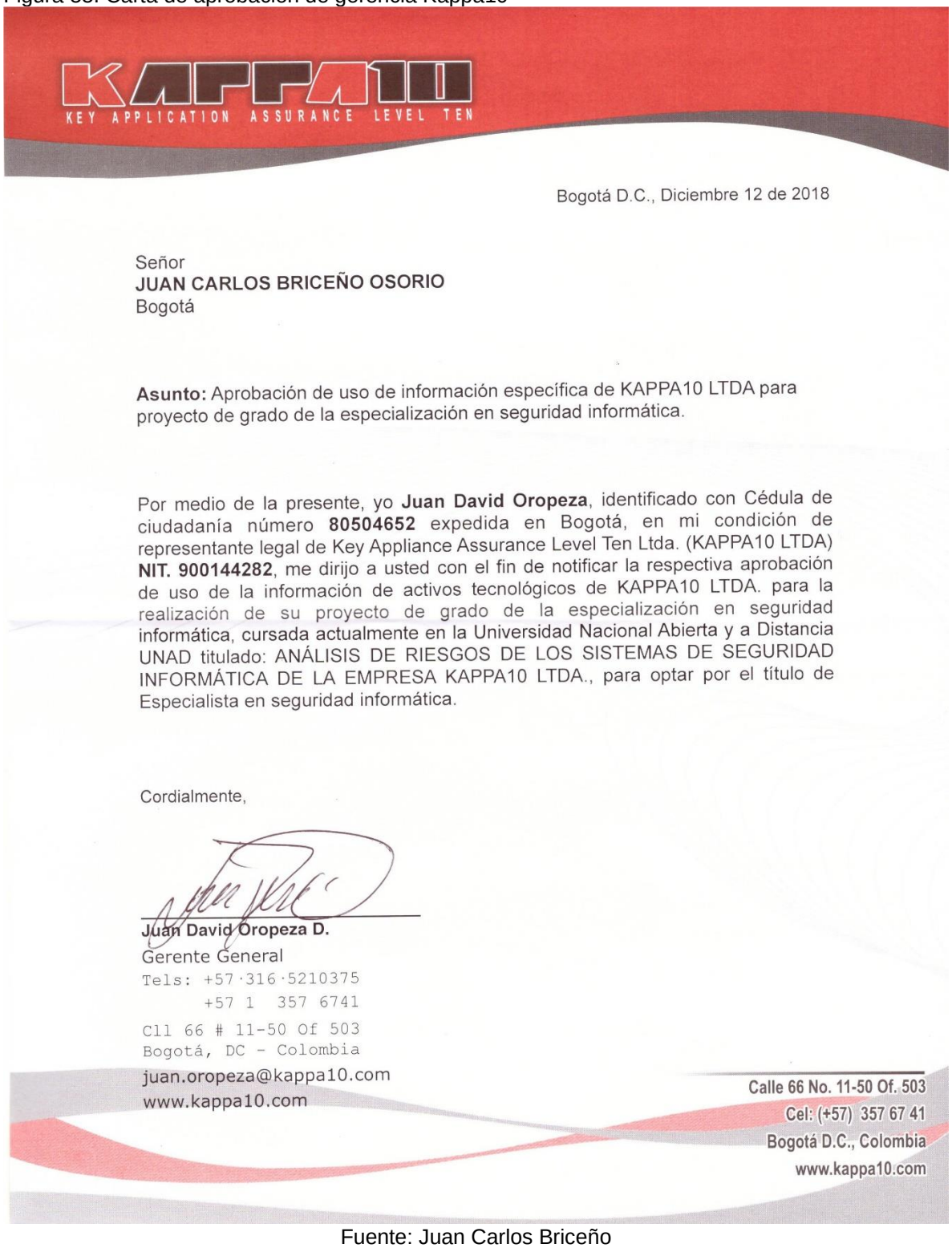
**JUAN CARLOS BRICEÑO OSORIO**
CC. 80933216 de Bogotá

Firma de aceptación Kappa10 Ltda.

**JUAN DAVID OROPEZA**

Fuente: Juan Carlos Briceño

Figura 55. Carta de aprobación de gerencia Kappa10



KAPPA10
KEY APPLICATION ASSURANCE LEVEL TEN

Bogotá D.C., Diciembre 12 de 2018

Señor
**JUAN CARLOS BRICEÑO OSORIO**
Bogotá

**Asunto:** Aprobación de uso de información específica de KAPPA10 LTDA para proyecto de grado de la especialización en seguridad informática.

Por medio de la presente, yo **Juan David Oropeza**, identificado con Cédula de ciudadanía número **80504652** expedida en Bogotá, en mi condición de representante legal de Key Appliance Assurance Level Ten Ltda. (KAPPA10 LTDA) **NIT. 900144282**, me dirijo a usted con el fin de notificar la respectiva aprobación de uso de la información de activos tecnológicos de KAPPA10 LTDA. para la realización de su proyecto de grado de la especialización en seguridad informática, cursada actualmente en la Universidad Nacional Abierta y a Distancia UNAD titulado: ANÁLISIS DE RIESGOS DE LOS SISTEMAS DE SEGURIDAD INFORMÁTICA DE LA EMPRESA KAPPA10 LTDA., para optar por el título de Especialista en seguridad informática.

Cordialmente,

**Juan David Oropeza D.**
Gerente General
Tels: +57·316·5210375
+57 1 357 6741
Cll 66 # 11-50 Of 503
Bogotá, DC - Colombia
juan.oropeza@kappa10.com
www.kappa10.com

Calle 66 No. 11-50 Of. 503
Cel: (+57) 357 67 41
Bogotá D.C., Colombia
www.kappa10.com

Fuente: Juan Carlos Briceño