DISEÑO DE POLÍTICAS DE CONTROL DE ACCESO Y ROBUSTECIMIENTO DE LA SEGURIDAD MEDIANTE LA INTEGRACIÓN DEL DIRECTORIO ACTIVO JUNTO A LA IMPLEMENTACIÓN DE SEGUNDO FACTOR DE AUTENTICACIÓN PARA LOS USUARIOS VPN DE LA EMPRESA B2B

DANILO ALFONSO ARIAS CARREÑO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2021

DISEÑO DE POLÍTICAS DE CONTROL DE ACCESO Y ROBUSTECIMIENTO DE LA SEGURIDAD MEDIANTE LA INTEGRACIÓN DEL DIRECTORIO ACTIVO JUNTO A LA IMPLEMENTACIÓN DE SEGUNDO FACTOR DE AUTENTICACIÓN PARA LOS USUARIOS VPN DE LA EMPRESA B2B

DANILO ALFONSO ARIAS CARREÑO

Proyecto de Grado presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Director del proyecto:
Ing. Edgar Roberto Dulce

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2021

NOTA DE ACEPTACIÓN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá, Fecha sustentación

DEDICATORIA

A mi esposa por su comprensión y apoyo, a mi hija por ceder tiempo y brindarme los espacios necesarios para el desarrollo de mis actividades académicas, a la Universidad Nacional Abierta y a Distancia UNAD por permitirme hacer parte de los aspirantes a especialistas en seguridad informática y brindarme el acompañamiento necesario para la elaboración de mi trabajo de grado.

AGRADECIMIENTOS

A Dios por mantener a mi familia unida y gozando de salud.

A mi familia por el apoyo y compresión constante.

A los docentes de la Universidad Nacional Abierta y a Distancia UNAD, por brindarme su apoyo y acompañamiento durante el proceso de formación de Especialista en Seguridad informática.

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

pág.

GLOSARIO

ACTIVO: Cada uno de los recursos físicos y lógicos con los que cuenta una organización para procesos de comunicación (bases de datos, servidores, routers, firewalls, programas, racks etc.)

AMENAZA: Cualquier evento, fenómeno o situación que pueda causar daño

ANÁLISIS DE RIESGO: Conjunto de procesos para identificar y comprender la naturaleza del riesgo y determinar sus niveles.

AUTENTICACIÓN: Proceso que debe seguir un usuario para identificarse en un sistema.

IMPACTO: Daño producido por la materialización de una amenaza.

ISO: Organización Internacional de Normalización. Es una agrupación de entidades nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares, (normas)[1]

[1] ISO 27000.ES. El portal de ISO 27001 en español [en línea]. Madrid: El autor, s.f. [citado el 22-04-16]. Disponible en: http://www.iso27000.es/iso27000.html

ISO/IEC 27001:2013: Norma internacional que establece los lineamientos y requisitos para un sistema de gestión de la seguridad de la información (SGSI). La versión 2013 corresponde a su segunda edición.

LDAP: Protocolo ligero de Acceso a directorios, es de tipo cliente – servidor para el ingreso al directorio, se utiliza para la autenticación y autorización de usuarios de una organización en el dominio.

POLÍTICA DE SEGURIDAD: Serie de lineamientos y procesos documentados que brindan las pautas para el aseguramiento de los activos de la compañía.

RIESGO: Probabilidad de que una amenaza ocurra.

RIESGO RESIDUAL: Riesgo remanente en el sistema después del tratamiento del riesgo.

SEGURIDAD INFORMÁTICA: Conjunto de técnicas para asegurar los activos de información de una compañía.

VULNERABILIDADES: Fallas de despliegue y aseguramiento de los sistemas que puedan ocasionar daño a la compañía.[2]

CONFIDENCIALIDAD: Privacidad, se refiere a que la información solo pueda ser consultada por personas autorizadas.

[2] Francisco Nicolás Solarte Solarte, Edgar Rodrigo Enríquez Rosero, y Mirian del Carmen Benavides, «Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001», Revista Tecnológica -ESPOL28, n.o5 (31 de diciembre de 2015), http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456

INTEGRIDAD: Característica de la información de estar intacta en su origen, a menos que personal autorizado realice modificaciones.

DISPONIBILIDAD: Característica de la información de estar siempre en línea disponible para ser consultada

MAGERIT: Metodología enfocada a proceso de gestión de los riesgos, se basa en la implementación de procesos de gestión del riesgo dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones tomando en cuenta los riesgos derivados del uso de las tecnologías de información.[3]

[3] Portal Administración Electrónica. MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información [recurso en línea] 2018. [Consultado el 1 de octubre de 2020] Disponible en internet: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WwGBZUiFPIU

RESUMEN

En base a las falencias de seguridad generadas por ingresos no autorizados de los ingenieros que hacen parte de la compañía B2B TIC SAS los cuales cuentan con el beneficio de teletrabajo, y con el fin de evitar robo de información como el ocurrido en compañías como Renault[4], se plantea en el presente proyecto el diseño de políticas específicas para el control de acceso vía VPN y el aumento en los niveles de seguridad mediante la adición de una segunda capa de autenticación de la mano con la Integración del directorio activo para los usuarios VPN de la empresa B2B TIC SAS con el fin de fortalecer la seguridad informática para el entorno de teletrabajo.

El proyecto hace uso de las características de la Infraestructura actual, consiste en un Firewall de seguridad perimetral de marca Fortinet que cuenta con integración al directorio activo por medio de LDAP, junto a él se cuenta con un servidor Windows Server 2016 que maneja el rol de directorio activo, controlando a los usuarios y equipos pertenecientes al dominio de la compañía.

Al culminar el proyecto la empresa B2B TIC SAS recibirá la documentación correspondiente a las políticas y procedimientos diseñados de control de acceso para usuarios VPN, con el fin de que se adhieran a su documentación interna y sean socializadas en la compañía, de igual forma se realizara la adición de nuevas capas para la autenticación de los usuarios VPN por medio de tokens y directorio activo, proceso que será documentado con su correspondiente paso a paso para su administración y solución de fallas que se llegaran a presentar posterior a la ejecución.

[4] EUROPA PRESS. Renault asegura que no se ha comprometido información esencial en el robo de datos. En:rtve.[En línea]. (8, enero 2011). Disponible en: https://www.rtve.es/noticias/20110108/renault-asegura-no-se-comprometido-informacion-esencial-robo-datos-compania/393539.shtml

ABSTRACT

Based on the security shortcomings generated by unauthorized income of the engineers who are part of the B2B TIC SAS company, which have the benefit of teleworking, and in order to avoid information theft such as occurred in companies like Renault, In this project, the design of specific policies for access control via VPN and the increase in security levels are proposed by adding a second layer of authentication in conjunction with Active Directory Integration for VPN users of the B2B TIC SAS company in order to strengthen computer security for the telework environment.

The project makes use of the characteristics of the current infrastructure, which consists of a Fortinet brand perimeter security firewall which allows integration processes to the active directory through LDAP, together with it there is a Windows Server 2016 server that manages the active directory role, controlling the users and computers belonging to the company domain.

At the end of the project, the B2B TIC SAS company will receive the documentation corresponding to the policies and procedures designed for access control for VPN users, in order to adhere to their internal documentation and be socialized in the company, in the same way it will be carried out the addition of new layers for the authentication of the VPN users by means of tokens and active directory, a process that will be documented with its corresponding step-by-step for its administration and solution of failures that will be presented after the execution.

INTRODUCCIÓN

El presente proyecto aplicado presenta el diseño de políticas de control de acceso para robustecer la seguridad junto a la implementación de un doble factor de autenticación e integración del directorio activo para la conexión de los usuarios vía VPN SSL, con el objetivo de aumentar los niveles seguridad informática para escenarios de teletrabajo para la empresa B2B TIC SAS y mitigar las vulnerabilidades asociadas.

La propuesta tiene como base el uso de la infraestructura actual, donde se cuenta con un Firewall de nueva generación Fortigate protegiendo el perímetro mediante los respectivos módulos de UTM y funcionando como terminador VPN para las conexiones cliente a sitio de tipo SSL, al incluir además la función de autenticación para 5 usuarios locales configurados correspondientes a los ingenieros, junto al firewall en la conexión a la interface DMZ existe un servidor de directorio activo en el cual se realiza el despliegue de todas las directivas de grupo y además se tiene el registro de cada uno de los equipos que pertenecen a la compañía B2B TIC SAS.

De igual manera se hace la identificación de los controles según la norma de seguridad de la información ISO 27001:2013 respecto al uso de dispositivos y conexiones para el transporte seguro de información, junto con el acceso de los usuarios a fin diseñar políticas acordes al estado actual de la compañía.

Dentro del desarrollo del proyecto se utiliza la metodología aplicada haciendo uso de técnica de recolección de información (entrevistas semiestructuradas) estas con el fin de generar un análisis para posteriormente solucionar la problemática identificada.

Estas entrevistas cuentan con 3 fases principales, entre las cuales están la fase de

inicio o rapport (*) durante la cual se crea un clima de confianza sin tener excesiva formalidad logrando naturalidad y espontaneidad por parte del entrevistado. La segunda fase llamada desarrollo, es donde se realizan las preguntas iniciando por las generales, pasando por complejas, sensibles para terminar con un resumen.[5] Por último, está la fase de cierre donde se realizan las preguntas en un tono más conciliador, con el ánimo de tener un repaso generar a fin de tratar de identificar temas no tratados y poder culminar la entrevista correspondiente.[6]

Posterior a la recolección y análisis de la información el resultado obtenido servirá para definir las políticas de control de acceso, también para fortalecer la seguridad informática en escenarios de teletrabajo y así lograr un impacto positivo en el control de seguridad Informática en la compañía B2B TIC SAS.

El proyecto aplicado ayudará a fortalecer mi conocimiento en el área de seguridad informática y lograr obtener el título de especialista de seguridad informática que ofrece la Universidad Nacional Abierta y a Distancia UNAD. También servirá como base de conocimiento para los futuros aspirantes a Ingenieros o especialistas (informática, telecomunicaciones, electrónica, seguridad informática, seguridad de la información) y quedará en el repositorio de la Universidad Nacional Abierta y a Distancia UNAD.

(*) Rapport: Palabra de origen Frances que significa crear una relación, término utilizado para nombrar el inicio o primera fase de una entrevista

[5] MORGA, Luis. (2012). Teoría y técnica de la entrevista. México: RED TERCER MILENIO S.C. {en línea}. {Consultado mayo de 2020}. Disponible en: http://www.aliat.org.mx/BibliotecasDigitales/salud/Teoria_y_tecnica_de_la_entrevista.pdf

[6] Ibid., p.21

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

La empresa B2B TIC SAS de orden privado es una pyme creada en el 2016, está radicada en Bogotá, principalmente cuenta con tres líneas de negocio, como lo son:

1. Distribución de productos de tecnología.
2. Desarrollo de software.
3. Profesionales de IT tercerizados.

Entre los clientes se destacan CenturyLink (**), Tigo (***), Sonda (****) y ETB (*****), actualmente tiene contratados 15 Ingenieros, 10 de ellos realizan sus labores en las instalaciones de la compañía y otros 5 trabajan mediante la figura de teletrabajo (los 15 ingenieros se rotan el teletrabajo) utilizando conexiones VPN SSL para la conexión a los entornos de desarrollo y producción.

La compañía durante la recepción de los reportes de acceso de usuarios VPN ha evidenciado accesos sobre horas no laborales, para lo cual los ingenieros que realizan el teletrabajo han hecho sus descargos indicando que ninguno de ellos es responsable de los accesos.

Las conexiones realizadas fuera del horario podrían estar acompañadas a robo de información en las compañías, como es el caso de Renault fabricante de autos francés donde se produjo un robo y filtración de información correspondiente al desarrollo de sus automóviles eléctricos nuevos de alto perfil los cuales estaban siendo trabajados en conjunto con Nissan, la compañía posterior a las investigaciones realizadas indico que se trata de un colectivo internacional con

(**) CenturyLink: compañía colombiana que brinda servicios de soluciones de red
(***) Tigo: Operador de telefonía móvil y de servicios de soluciones de red
(****) Sonda: Operador de soluciones integrales de tecnología
(*****) ETB: Empresa de Telecomunicaciones de Bogotá, proveedor de soluciones de red

intereses económicos, tecnológicos y estratégicos los cuales fueron apoyados por trabajadores de Renault, quienes fueron apartaron de sus cargos. [7]

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo el diseño de políticas de control de acceso y una segunda capa de autenticación para los usuarios VPN pueden fortalecer la seguridad de la información e informática en escenarios de teletrabajo para la empresa B2B TIC SAS?

[7] EUROPA PRESS. Renault asegura que no se ha comprometido información esencial en el robo de datos. En:rtve.[En línea]. (8, enero 2011). Disponible en: https://www.rtve.es/noticias/20110108/renault-asegura-no-se-comprometido-informacion-esencial-robo-datos-compania/393539.shtml

2 JUSTIFICACIÓN

Hoy en día con el fin de mejorar la calidad de vida del trabajador y la posibilidad del uso de las tecnologías se implementa la modalidad del teletrabajo que además de ser una forma eco-amigable de trabajo, genera impactos positivos sobre los empleados y empleadores siendo una alternativa beneficiosa para ambas partes. Como lo indica el libro blanco el abc del teletrabajo en Colombia.[8]

A su vez teniendo un impacto sobre el desarrollo sostenible, como lo son objetivo de trabajo decente, crecimiento económico, producción y consumo responsable. Dado a que el teletrabajo es un instrumento que debidamente enfocado impulsa el crecimiento empresarial, al brindar la posibilidad de ofrecer trabajo bien remunerado, el cual es reflejado en la productividad de sus empleados, esto apalancado por la reducción de los costos operativos de las instalaciones físicas de las empresas (mantenimiento, aseo, servicios públicos, alquiler etc), por tanto, reduciendo el uso de bienes y recursos.[9] Sin embargo, el teletrabajo debe ser abordado con mayor ahínco, debido a la seguridad, pues en este escenario se interactúa digitalmente, lo que en la actualidad implica cientos de riesgos, los cuales pueden convertirse en Amenazas latentes, que pueden lograr que las organizaciones presenten perdidas en activos de información, productividad, daños en reputación, con consecuencias económicas y o legales.[10]

[8] MINISTERIO DEL TRABAJO, Libro blanco El abc del teletrabajo en Colombia [En línea]. Bogotá: Ministerio del Trabajo.2015., 97 p Disponible en https://www.teletrabajo.gov.co/622/articles-8228_archivo_pdf_libro_blanco.pdf

[9] PNUD, ODS en Colombia; Los retos para 2030[En línea]. Bogotá: Programa de las naciones unidas para el desarrollo PNUD .2018., 74 p Disponible en https://www.undp.org/content/dam/colombia/docs/ODS/undp_co_PUBL_julio_ODS_en_Colombia_los_retos_para_2030_ONU.pdf

[10] CCIT y POLICIA, Tendencias cibercrimen Colombia 2019 - 2020. Bogotá: CCIT, 2019. [En línea]. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Diseñar políticas específicas para el control de acceso vía VPN y aumentar los niveles de seguridad mediante la adición de una segunda capa de autenticación junto con la Integración del directorio activo para los usuarios VPN de la empresa B2B TIC SAS fortaleciendo la seguridad informática para el teletrabajo.

3.2 OBJETIVOS ESPECÍFICOS

- Determinar el estado actual de la seguridad informática de la empresa B2B TIC SAS mediante un análisis de riesgos.

- Integrar el directorio activo de la compañía B2B TIC SAS al firewall perimetral por medio de LDAP, para fortalecer y generar seguimiento de las conexiones VPN SSL de los ingenieros de la compañía.

- Definir las políticas de seguridad para el control de acceso de los usuarios vía VPN, con el fin de que sean documentadas y socializadas en el respectivo proceso de inducción del personal nuevo o reinducción de los ya existentes.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

4.1.1 Seguridad de la información. Asegurar entornos empresariales para lograr la implementación del teletrabajo acarrea procesos, los cuales deben estar en mejora continua según las políticas específicas diseñadas para tal fin y cubiertas por la legislación en materia de protección de datos, así como tener presentes los lineamentos generales como se observa en el libro blanco el abc del teletrabajo en Colombia sobre el anexo 3 artículo 10 sobre el cual se indica:

La empresa brindará las herramientas específicas (hardware/software) que considere necesarias para el desarrollo de las funciones e implementará las correspondientes medidas de control y acceso, con el fin de garantizar la protección de datos y de los mismos equipos y aplicaciones entregadas. De igual forma, el teletra-bajador deberá respetar lo contemplado en las leyes colombianas, así como las instrucciones por escrito que reciban de sus supervisores o jefes inmediatos.

El teletrabajador no podrá comunicar a terceros, salvo autorización expresa y escrita del empleador, o por orden de las autoridades competentes, la información que tenga sobre su trabajo, cuyo origen provenga del uso de tecnologías de la información que le haya suministrado su empleador, especialmente sobre los asuntos que sean de naturaleza reservada y/o cuya divulgación pueda ocasionar perjuicios a la empresa o a las personas a quienes se les presta el servicio, lo que no obsta para denunciar delitos comunes o violaciones del contrato o de las normas legales de trabajo ante las autoridades competentes.

De igual forma, el teletrabajador no podrá compartir los usuarios y/o contraseñas personales de la empresa que le hayan sido entregados con ocasión del teletrabajo contratado.

El teletrabajador deberá conservar, mantener y devolver en buen estado, salvo deterioro natural y razonable, en el momento en que la empresa lo solicite, los instrumentos, equipos informáticos y los útiles que se le haya facilitado para la prestación de sus servicios.[11]

El teletrabajo se define en la ley 1221 de 2008 como “una forma de organización laboral, que consiste en el desempeño de una actividad remunerada o prestación de servicios a terceros utilizando como soporte las tecnologías de la información y comunicación -TIC- para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio específico de trabajo”[12]

Con respecto al teletrabajo este debe venir acompañado de la seguridad por medio de alguno de los modelos de seguridad de la información, entre los cuales están NIST 2012, COBIT 5 y ISO 27001:2013 que se describirán a continuación:

NIST el cual es una metodología de gestión de riesgo, proporcionada en forma de guía, desarrollada por el departamento de comercio del gobierno de los Estados Unidos. El Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST) implemento la guía: Seguridad de la información para pequeñas empresas, que tiene como objetivo proporcionar recomendaciones de seguridad cibernética básicas para empresas a través de un proceso de evaluación de riesgos.

Al proporcionar liderazgo técnico para la infraestructura nacional de medición y

[11] MINISTERIO DEL TRABAJO, Libro blanco El abc del teletrabajo en Colombia [En línea]. Bogotá: Ministerio del Trabajo.2015., 97 p Disponible en https://www.teletrabajo.gov.co/622/articles-8228_archivo_pdf_libro_blanco.pdf
[12] Ibid., p. 6.

estándares, NIST SP 800-30 desarrolla técnicas de prueba, datos de referencia, pruebas de implementaciones conceptuales y análisis técnicos para avanzar en el desarrollo y el uso productivo de la tecnología de la información. NIST contiene el desarrollo de normas y directrices técnicas, físicas, administrativas y de gestión para la seguridad y privacidad adecuada de la información delicada no clasificada en sistemas informáticos federales. La publicación especial 800-series informa sobre los esfuerzos de investigación, orientación y divulgación de NIST en seguridad informática, y sus actividades de colaboración con la industria, el gobierno y las organizaciones académicas. La guía está conformada por cinco secciones que en conjunto son un proceso iterativo de tareas que se ejecutan de manera secuencial.

La metodología propuesta por NIST SP 800-30, incluye los siguientes subprocesos: (Sotelo Bedón, Torres Utrilla et al. 2012) [13]

- Caracterización de sistemas.
- Identificación de amenazas y vulnerabilidades.
- Análisis de controles.
- Determinación de probabilidades.
- Análisis de impacto.
- Determinación del riesgo.
- Recomendaciones de controles.
- Documentación de resultados.

COBIT 5 es un marco de referencia para la gestión de tecnologías de la información, elaborado por ISACA (Asociación de Control y Auditoria de Sistemas de Información), que facilita a las organizaciones nivelar los beneficios de la realización corporativa con niveles reducidos de riesgos y uso de recursos.

[13] LARA GUIJARRO, Elva Gioconda; CORELLA GUERRA, Flavio Aníbal. Comparación de modelos tradicionales de seguridad de la información, Tierra Infinita**,** [S.l.], v. 4, n. 1, p. 20-28, dic. 2018. Disponible en: http://revistasdigitales.upec.edu.ec/index.php/tierrainfinita/article/view/74

Su enfoque se basa en el desarrollo de políticas y mejores prácticas de seguridad en el manejo de la información de la compañía. [14]

COBIT se encuentra dividido en cuatro dominios:

• Planear y organizar.
• Adquirir e implementar.
• Distribuir y dar soporte.
• Monitorear y evaluar.

ISO 27001:2013 es una norma internacional, diseñada por la ISO (international Organization for Standardization), su función es brindar los lineamientos y requisitos para implementar un SGSI (sistema de gestión de seguridad informática) y detalla cómo realizar la gestión de la seguridad de la información en un entorno empresarial, la ISO 27001:2013 aplica a todo tipo de organizaciones sin importar su enfoque o tamaño.[15]

Entre su mayor beneficio en comparación con NIST y COBIT 5 se encuentra la forma de proveer metodologías de implementación y su enfoque hacia cualquier tipo de entorno empresarial, junto con sus completos controles de seguridad, en base a ello será la norma utilizada para la definición de las políticas de control de acceso.

La norma al ser aplicada permite una reducción o eliminación de incidentes de seguridad, y debido al manejo del ciclo phva (planear hacer verificar actuar), genera que el sistema sea constantemente evaluado y se ajuste a las nuevas necesidades, es por esto que muchas entidades gubernamentales como por ejemplo la Dian bajo

[14] LARA GUIJARRO, Elva Gioconda; CORELLA GUERRA, Flavio Aníbal. Comparación de modelos tradicionales de seguridad de la información, Tierra Infinita**,** [S.l.], v. 4, n. 1, p. 20-28, dic. 2018. Disponible en: http://revistasdigitales.upec.edu.ec/index.php/tierrainfinita/article/view/74

[15] OLIVAN HUERVA, Antonio. Guía de controles de ciberseguridad para la protección integral de la pyme [En línea].Bogotá:Antonio Olivan Huerva.2017., 124 p. Disponible en http://openaccess.uoc.edu/webapps/o2/bitstream/10609/73066/6/aolivan1TFM0118memoria.pdf

su decreto 2242/2015 emitió un comunicado, listando entre los requisitos para las empresas que quieran ser sus proveedores que deben estar certificados bajo la norma ISO 27001:2013, de forma que las empresas para poder ser competitivas deberán realizar la implantación y certificación en ISO 27001:2013 por medio de las entidades avaladas para dicho fin como bureau veritas.[16]

ISO 27001:2013 esta principalmente enfocado en proteger la confidencialidad, integridad y disponibilidad de la información de las organizaciones, y consta de 144 controles de seguridad, 14 dominios y 35 objetivos de control, para lo cual existe un documento llamado anexo A, donde se hacen referencia a cada uno de ellos.[17]
Uno de los principales dominios para la ejecución de la presente propuesta es el dominio 9 que corresponde a Gestión de los controles de acceso, el cual según ISO 27001:2013 hace referencia a *"*Los usuarios solo deben tener acceso a la red y a los servicios para los que se les ha autorizado específicamente para usar. El acceso debe ser controlado por un procedimiento de inicio seguro y restringido, de acuerdo con la política de control de acceso"*[18]*

Se divide en 4 objetivos de control:

9.1 Requisitos de negocio para el control de acceso
9.2 Gestión de Acceso de usuario
9.3 Responsabilidad del usuario
9.4 Control de acceso a sistemas y aplicaciones.

[16] MINISTERIO DE HACIENDA Y CREDITO PUBLICO. Decreto número 2242 de 2015 [En línea]. Bogotá: presidente de la república de Colombia., 19 p. Disponible en https://www.dian.gov.co/fizcalizacioncontrol/herramienconsulta/FacturaElectronica/Factura%20Electrnica/Decreto_2242_del_24_de_Noviembre_2015.pdf
[17] ISOTOOLS EXCELLENCE.La norma ISO 27001: Aspectos claves de su diseño e implantación [En línea].Bogotá: isotools.2020., 23 p. Disponible en https://www.isotools.org/pdfs-pro/iso-27001-sistema-gestion-seguridad-informacion.pdf
[18] HURTADO PEREZ, Andres Julian.Diseño del sistema de gestión de seguridad de la informacion [En línea].Bogotá:Jaime Andres Julian Hurtado Perez .2017., 239 p. Disponible en http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6433/SGSI%20-%20FEBOR%20-%20Trabajo%20de%20Grado.pdf?sequence=2&isAllowed=y

Cada uno de los Objetivos de control listados anteriormente cuentan con sus debidos controles los cuales se encuentran documentados sobre el Anexo A de la norma ISO 27001:2013, los cuales son descritos sobre el Anexo 1.

4.1.2 Análisis y gestión de Riesgos. Para cualquier compañía que haga uso de la tecnología es necesario que tenga conocimiento de los riesgos inherentes al uso de esta, generalmente el riesgo solo es planteado como una amenaza, determinando el grado de exposición a la ocurrencia de un evento que genere una perdida.

Para la Organización internacional por la normalización ISO se da una definición de riesgo tecnológico como “La probabilidad de que una amenaza se materialice, utilizando vulnerabilidad existente de un activo o un grupo de activos, generándole perdidas o daños”[19], en ella se identifican varios conceptos como probabilidad de amenaza, vulnerabilidades, activos e impacto.

El análisis de riesgo es una herramienta de diagnóstico que ayuda a establecer la exposición real a los riesgos a los que está expuesta una organización. El análisis tiene como principal objetivo identificar los riesgos en base a los activos de la organización, logrando establecer valores para el riesgo total y posteriormente el residual, el cual es resultado del tratamiento del riesgo aplicando las contramedidas correspondientes.

El valor del riesgo total es una agrupación de los elementos que lo conforman, calculando el valor del impacto por la probabilidad de la ocurrencia de la amenaza y cuál es el activo que ha sido impactado. Matemáticamente para la combinación de activo y amenaza la ecuación seria:

[19] INTERNATIONAL ORGANIZATION FOR STANDARIZATION. ISO/IEC 13335-1:2004 [ISO/IEC 13335-1:2004]. Suiza:2004. [fecha de consulta: 17 de octubre de 2019]. Disponible en: https://www.iso.org/standard/39066.html

RT (riesgo total) = probabilidad x impacto

Para el análisis de riesgo generalmente se utiliza un documento llamado matriz de riesgo, en donde se encuentran los activos identificados, la relación los cálculos ejecutados. La sumatoria de riesgo residual, es la exposición de la compañía a los riesgos.
El análisis de riesgo se basa principalmente en los activos de la compañía, de esta forma logrando identificar las causas potenciales de los riesgos que amenazan el entorno de la compañía. La información de los activos de la compañía debe ser lo más veraz posible por lo que se recomienda tener el máximo detalle de cada uno de ellos.

El análisis de riesgo viene acompañado de tareas importantes en cuanto al análisis, tiempo y recursos disponibles para atacar los problemas, y generar un análisis minucioso de los riesgos y debilidades, obteniendo la identificación y logrando generar los respectivos controles o procesos de mitigación a la medida de la compañía.

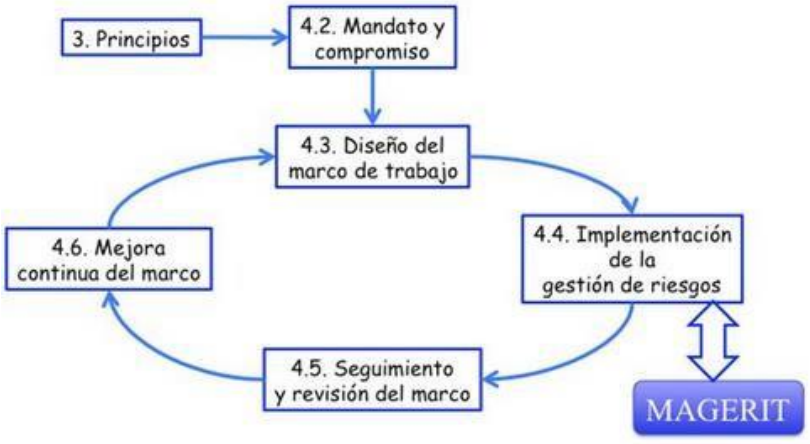
Para abordar el análisis de riesgo se cuentan con distintas metodologías, las cuales son una guía paso a paso para ejecutar las acciones propias de cada una de ellas y obtener el respectivo análisis de riesgo, permitiendo un enfoque claro para abordar el problema de una forma total, sistemática y disciplinada.

A continuación, se explica las metodologías de análisis de riesgo; las cuáles según el listado de INCIBE son las más recomendadas por su completa documentación y fácil aplicación, entre ellas están MAGERIT, CRAMM Y OCTAVE.

4.1.2.1 Magerit. Es una metodología de análisis y gestión de riesgo de los sistemas de información, elaborada por el consejo superior de Administración electrónica de España que hoy en día se conoce como comisión de estrategia TIC, nace como respuesta a la percepción de que la administración y en general, toda la sociedad, dependen de forma creciente de las tecnologías de información para el cumplimiento de su misión.[20]

Conocer el riesgo al que se someten los activos de una organización es imprescindible para poder gestionarlos de una madera adecuada, por ello sobre la metodología se implementa el proceso de gestión de riesgo dentro de un marco de trabajo el cual se basa en diseño, implementación, revisión y mejora continua como se observa en la Figura 1. Con MAGERIT se persigue una aproximación metódica que no deje lugar a improvisación, ni dependa del análisis.[21]

Figura 1. Marco de trabajo para la gestion de riesgo



Fuente: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

[20] Portal Administración Electrónica. MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información [recurso en línea] 2018. [Consultado el 1 de octubre de 2020] Disponible en internet: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WwGBZUiFPIU8567-2d44b3020387/2012_Magerit_v3_libro1_metodo_es_NIPO_630-12-171-8.pdf, pág. 7

[21] Ibid., p.2

MAGERIT mediante la gestión de riesgo abarca el análisis de los riesgos asociados a los activos de información evaluando el impacto que una violación de la seguridad tiene en la organización, señalando riesgos existentes, identificando amenazas de los sistemas de información, y posterior a este análisis se realiza el tratamiento de los riesgos realizando la implementación de salvaguardas según las necesidades de la organización.

En la actualidad MAGERIT se encuentra en su Versión 3 y se encuentra estructurada en dos libros y una guía técnica: Libro I Método, Libro II Catálogo de elementos y Guía técnica, a continuación, una breve explicación de cada una de ellas.

El Libro I método describe los pasos y las tareas básicas para realizar un proyecto de análisis y gestión de riesgos, y proporciona una serie de aspectos prácticos, este cuenta con la siguiente estructura:

- El capítulo 2 presenta los conceptos informalmente. En particular se enmarcan las actividad-des de análisis y tratamiento dentro de un proceso integral de gestión de riesgos.

- El capítulo 3 concreta los pasos y formaliza las actividades de análisis de los riesgos.

- El capítulo 4 describe opciones y criterios de tratamiento de los riesgos y formaliza las actividades de gestión de riesgos.

- El capítulo 5 se centra en los proyectos de análisis de riesgos, proyectos en los cuales se debe estar inmerso para realizar el primer análisis de riesgos de un sistema y eventualmente cuando hay cambios sustanciales poder rehacer el modelo.

- El capítulo 6 formaliza las actividades de los planes de seguridad, a veces denominados planes directores o planes estratégicos.

- El capítulo 7 se centra en el desarrollo de sistemas de información y cómo el análisis de riesgos sirve para gestionar la seguridad del producto final desde su concepción inicial hasta su puesta en producción, así como a la protección del propio proceso de desarrollo.

• El capítulo 8 se anticipa a algunos problemas que aparecen recurrentemente cuando se realizan análisis de riesgos.[22]

El Libro II Catálogo de elementos ofrece unas pautas y elementos estándar en cuanto a: tipos de activos, dimensiones de valoración de los activos, criterios de valoración de los activos, amenazas típicas sobre los sistemas de información y salvaguardas a considerar para proteger sistemas de información, principalmente persigue dos objetivos esenciales: el facilitar la labor de las personas que inician el proyecto, en el sentido de ofrecerles elementos estándar a los que puedan adscribirse rápidamente, centrándose en lo específico del sistema objeto del análisis y homogeneizar los resultados de los análisis, promoviendo una terminología y unos criterios uniformes que permitan comparar e incluso integrar análisis realizados por diferentes equipos, este libro cuenta con la siguiente estructura:

• El capítulo 2 presenta los conceptos de tipos de activos

• El capítulo 3 concreta las dimensiones de valoración de los activos

• El capítulo 4 describe los criterios de valoración de los activos

• El capítulo 5 se centra en las diferentes amenazas

• El capítulo 6 se centra en las salvaguardas [23]

[22] Portal Administración Electrónica. MAGERIT v.3: MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I – Método [recurso en línea] 2018. [Consultado el 1 de octubre de 2020] Disponible en internet: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WwGBZUiFPIU

[23] Portal Administración Electrónica. MAGERIT v.3: MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II - Catálogo de Elementos [recurso en línea] 2018. [Consultado el 1 de octubre de 2020] Disponible en internet: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WwGBZUiFPIU

La guía técnica, es una guía de consulta que presenta técnicas empleadas habitualmente para la ejecución de proyecto de análisis y gestión del riesgo, análisis mediante tablas, árboles de ataque, técnicas generales, análisis de algoritmos, diagrama de flujos de datos, diagramas de procesos, planificación de proyectos entre otras, y está compuesta por:

- El capítulo 2 Técnicas específicas
- El capítulo 3 Técnicas generales [24]

4.1.2.2 Cramm. Proviene del acrónico CCTA Risk Analysis and Management Method, su versión inicial fue lanzada sobre el año 1987 por la agencia central de comunicación y telecomunicación del gobierno británico, actualmente está en su versión 5.1.

Es el método de análisis de riesgos preferente en Organismos de la Administración Pública británica. El mantenimiento y la gestión de la metodología están a cargo de la empresa privada de consultoría Insight Consulting, actualmente integrada en Siemens.[25]

Uno de los aspectos principales de CRAMM es el soporte que proporciona la herramienta informática que la soporta, con una base de datos de:

- Más de 400 tipos de activos
- Más de 25 tipos de impacto

[24] Portal Administración Electrónica. MAGERIT v.3: MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro III - Guía de Técnicas [recurso en línea] 2018. [Consultado el 1 de Octubre de 2020] Disponible en internet: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WwGBZUiFPIU

[25] MATALOBOS VEIGA, Juan Manuel. Análisis de riesgos de seguridad de la información. Madrid: Universidad Politécnica de Madrid. Facultad de informática, 2009. 88 p

- 38 tipos de amenaza
- 7 tipos de medida del riesgo
- Más de 3.500 salvaguardas

Actualmente CRAMM cuenta con tres tipos de revisiones:

•CRAMM Express
•CRAMM Expert
•BS7799

La metodología CRAMM define tres fases para la realización del análisis de riesgos:

Fase 1: Establecimiento de objetivos de seguridad:

- Definir el alcance del estudio.
- Definir el valor de la información entrevistando a los usuarios sobre los impactos potenciales para el negocio que podrían producirse por la indisponibilidad, destrucción, divulgación o modificación.
- Identificar y evaluar los activos físicos que forman parte del sistema.
- Identificar y evaluar los activos de software que forman parte del sistema.

Fase 2: Evaluación de riesgos:

- Identificar y valorar el tipo y nivel de las amenazas que pueden afectar al sistema.
- Valorar las vulnerabilidades de los sistemas ante las amenazas identificadas.
- Combinar las valoraciones de amenazas y vulnerabilidades para calcular la medida de los riesgos.

Fase 3: Identificación y selección de contramedidas:

Los principales productos de la metodología CRAMM son:

- Documento de inicio del proyecto
- Informes de análisis de riesgos
- Informes de gestión de riesgos, basados en una base de datos de más de 3.500 salvaguardas técnicas y organizativas.
- Plan de implantación

4.1.2.3 Octave. Proviene del acrónimo Operationally Critical Threat, Asset and Vulnerability Evaluation. OCTAVE es un modelo para la creación de metodologías de análisis de riesgos desarrollado por la Universidad de Carnegie Mellon. Es una evaluación de riesgos estratégica y técnica de seguridad. OCTAVE es autodirigido, lo que significa que el personal vinculado debe asumir la responsabilidad de llevar a cabo su implementación dentro de la organización. [26]

La técnica aprovecha el conocimiento de los relacionados con los procesos para terminar el estado de seguridad actual dentro de la organización.

Cualquier metodología que aplique los criterios puede considerarse compatible con el modelo OCTAVE, y cuenta con tres metodologías publicadas, las cuales son:

- OCTAVE: La metodología original, definida para grandes organizaciones.
- OCTAVE-S: Metodología definida para pequeñas organizaciones.

[26] OCTAVE Method Implementation Guide.Carnegie Mellon University[on line].Pittsburgh Pensilvania.[fecha de consulta: 5 de Octubre de 2020]. Disponible en www.cert.org/octave/octavemethod.html

- OCTAVE Allegro: Metodología definida para analizar riesgos con un mayor enfoque en los activos de información, en oposición al enfoque en los recursos de información.

Los criterios que forman el núcleo de OCTAVE son:

La metodología debe ser autodirigida:

- RA.1 Equipo de análisis
- RA.2 Capacidades del equipo de análisis

Las medidas deben ser adaptables a las necesidades:

- RA.3 Catálogo de prácticas
- RA.4 Perfil genérico de amenazas
- RA.5 Catálogo de vulnerabilidades

El proceso debe ser definido:

- RA.6 Actividades de evaluación definidas
- RA.7 Documentación de los resultados de la evaluación
- RA.8 Alcance de la evaluación

El proceso debe ser continuo:

- RA.9 Próximos pasos
- RA.3 Catálogo de prácticas

El proceso debe seguirse con visión de futuro.

- RA.10 Enfoque en riesgos

El proceso debe centrarse en un reducido número de riesgos críticos:

- RA.8 Alcance de la evaluación
- RA.11 Actividades enfocadas

Gestión integrada:

- RA.12 Aspectos organizativos y tecnológicos
- RA.13 Participación de negocio y de áreas tecnológicas
- RA.14 Participación de la alta dirección

Comunicación abierta:

- RA.15 Enfoque colaborativo

Perspectiva global:

- RA.12 Aspectos organizativos y tecnológicos
- RA.13 Participación de negocio y de áreas tecnológicas

Equipo de trabajo

- RA.1 Equipo de análisis
- RA.2 Capacidades del equipo de análisis
- RA.13 Participación de negocio y de áreas tecnológicas
- RA.15 Enfoque colaborativo

Para cada metodología se define un conjunto de procesos diferente adaptado a las necesidades particulares, siempre cumpliendo todos los criterios. Los procesos de cada una de las metodologías son:

Fase 1: Visión organizativa

- RO1.1 Activos críticos
- RO1.2 Requerimientos de seguridad para los activos críticos
- RO1.3 Amenazas sobre los activos críticos
- RO1.4 Prácticas de seguridad actuales
- RO1.5 Vulnerabilidades organizativas actuales

Fase 2: Visión tecnológica

- RO2.1 Componentes claveo
- RO2.2 Vulnerabilidades tecnológicas actuales

Fase 3: Estrategia y desarrollo del plano

- RO3.1 Riesgos sobre activos críticos
- RO3.2 Medidas contra los riesgos
- RO3.3 Estrategia de protección
- RO3.4 Planes de mitigación del riesgo.

4.2 MARCO CONCEPTUAL

A continuación, se abordan los principales conceptos relacionados con la seguridad informática tratados en el presente proyecto aplicado, los cuales se manejan durante su ejecución.

- Amenazas: son aquellas acciones que ocasionan consecuencias negativas en las operaciones de las compañías. Generalmente se indican como amenazas a las fallas, los desastres ambientales como terremotos o inundaciones, a los virus, a los ingresos no autorizados, accesos no autorizados, uso inadecuado de software, facilidad de acceso a las instalaciones, etc.[27]

- Vulnerabilidad: debilidad del sistema informático a causa de configuraciones erróneamente aplicadas o a brechas de seguridad a nivel de software, que pueden ser usadas para causar un daño. Las vulnerabilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware como en el software [28]

- Control de acceso a la red: El Control de Acceso a la Red permite el control del acceso a red por parte de los usuarios, mediante la verificación del cumplimiento de las políticas de seguridad establecidas con lo que se pueda prevenir amenazas como la exposición a virus, la salida no autorizada de información, accesos no autorizados, entre otros. Sin, las empresas centran su estrategia de seguridad en la protección de los equipos de red y su información de atacantes externos, no dando la suficiente importancia a los

[27] SECURITY ARTWORK. Seguridad y riesgos en el tic [recurso en línea]. 2008. [Consultado el 11 de marzo de 2020]. Disponible en internet: https://www.securityartwork.es/2008/10/31/seguridad-y-riesgos-en-las-tic-ii/

[28] R. Shirey, " Internet Security Glossary.", May 2000. [Online]. Available: https://tools.ietf.org/html/rfc2828

elementos existentes en la red interna, por lo cual y si lo que se desea es mantener pleno control de la red es necesario la definición de un control de acceso a red (NAC), el cual permite realizar cuatro acciones principales[29]

- Firewall (cortafuego): Es un sistema de red que está encargado de separar redes informáticas, controlando el tráfico existente entre ellas. Este control permite o deniega el paso de la comunicación entre redes.[30]

- VPN (Virtual Private Network) es una tecnología que permite una extensión segura de la red local (LAN) sobre una red pública o no controlada como Internet, su principal función es brindar conexión a los usuarios remotos, con el fin de que puedan tener acceso a los recursos de la organización como si se encuentran ubicados en las instalaciones de la compañía. Las VPN utilizan un proceso de cifrado y encapsulación de los datos que cursan por allí, haciendo que la información viaje de una manera segura por un túnel.[31]

- Riesgo: comprende el impacto para una compañía y su entorno que podrían ocurrir en base a las amenazas y vulnerabilidades asociadas con la operación y el uso de los sistemas de información y la infraestructura tecnológica.[32]

- Seguridad: Es usado en el sentido de minimizar los riesgos a que están

[29] INGENIA. Control de acceso a red (NAC). [en línea] 2018. [Consultado: 20 de abril de 2020]. Disponible en internet: https://www.ingenia.es/es/servicio/control-de-acceso-red-nac

[30] LEON RIVEROS, Paula. Diseño de seguridad de firewall perimetral para la organización clínica Barraquer. [en línea]. Disponible en: https://repository.unad.edu.co/handle/10596/25634

[31] ALVAREZ DELGADO, Diego.Redes Privadas Virtuales [En línea]. Bogotá: Diego Álvarez Delgado.2014., 9 p. Disponible en http://profesores.elo.utfsm.cl/~agv/elo322/1s14/projects/reports/G20/Redes%20Privadas%20Virtuales%20%28VPN%29.pdf

[32] CORDERO MORENO, José Leonardoy GARCÍA REYES Yadimyr OswaldoAnálisis de riesgos y recomendaciones de seguridad de la información del hospital E.S.E. San Bartolomé de Capitanejo, Santander [On line], [consultado el 23 de septiembre de 2020]. Disponible en Internet: repository.unad.edu.co/handle/10596/6366

sometidos los bienes informáticos hasta llevarlos a niveles adecuados[33]

- Seguridad de la Información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad, no repudio y afinidad[34]

4.3 MARCO LEGAL

4.3.1 Ley 1273 de 2009 para Delitos Informáticos. En Colombia existe la ley 1273 de 2009 denominada "De la protección de la información y de los datos", nace el 5 de enero de 2009 por el congreso de la república, por la cual se modifica el código penal y se crea un nuevo mecanismo legal, cuyo objetivo es sancionar todo comportamiento ilícito frente a la comisión de los delitos informáticos en el país.

La ley cuenta con dos capítulos los cuales se encuentran compuestos con sus respectivos artículos y penas según su gravedad, en donde se tipifican cada una de las maniobras utilizadas por los atacantes para obtener, obstaculizar, interceptar, dañar, suplantar cualquier activo o información ajena a la que no se les haya autorizado, dichos capítulos y o artículos se listan sobre el Anexo 2 del presente trabajo.

Ley 1581 de 2012 para la Protección de Datos Personales. “Es la normatividad que establece los lineamentos para el tratamiento de la información y la protección

[33] Oficina de Seguridad para las Redes Informáticas, Metodología para la Gestión de la Seguridad Informática [En línea]. Disponible en https://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf
[34] SUAREZ, Heiner Políticas de seguridad [En línea]. Bogotá: Heiner suarez.2017.,57 p. Disponible en http://repository.udistrital.edu.co/bitstream/11349/8322/4/Anexo%20C%20-%20Politicas%20de%20seguridad.pdf

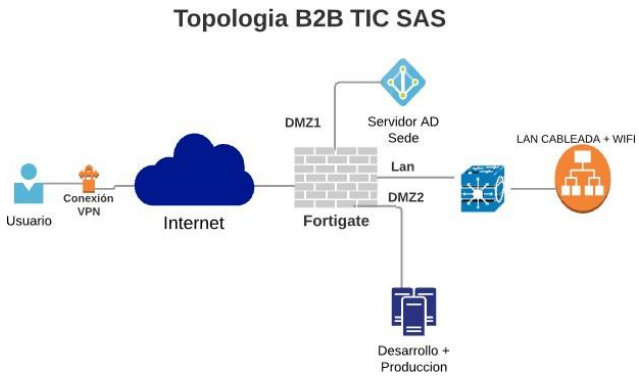
de los datos personales de los ciudadanos colombianos"[35]. Esta ley define los tipos de datos, responsables, mecanismos de vigilancia y control, así como procedimiento y sanciones en pro de proteger y resguardar los datos de los ciudadanos que han sido registrados en cualquier base de datos en el territorio nacional, además se protege de cualquier tipo de operación, recolección almacenamiento, uso, circulación o tratamiento por parte de organizaciones públicas y privadas. Su principal objetivo es garantizar privacidad de los datos y la intimidad a los colombianos, teniendo en cuenta la protección de los derechos fundamentales de la información personal, con base en el principio de confidencialidad para el buen uso de los datos personales e integridad para garantizar su estructura y sentido.[36]

4.4 MARCO METODOLÓGICO

En la compañía B2B TIC SAS, cuenta con una infraestructura de seguridad básica, en la cual se tiene actualmente un firewall de seguridad perimetral de nueva generación marca Fortinet con una versión de firmware 5.6.6, con características de UTM habilitadas. Dicho firewall tiene una conexión hacia un servidor de directorio activo Windows server 2016 el cual tiene el registro de todas las máquinas que hacen parte del dominio de la empresa y desde allí se aplican las distintas directivas de grupo y o actualizaciones correspondientes para el antivirus, adicional a dicha conexión tiene una hacia los servidores de desarrollo y producción, otra conexión hacia su red LAN compuesta por dos VLANS una para la red inalámbrica y otra para la red cableada, como se observa en la Figura 2.

[35] COLOMBIA. SECRETARIA DEL SENADO. Ley estatutaria 1581 de 2012, protección de datos personales. [En línea]. Disponible en Internet: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html.
[36] Ibíd., p. 2-35.

Figura 2. Topologia red B2B TIC SAS



Fuente: El Autor

A su vez el firewall tiene configurado el servicio de VPN cliente a sitio SSL para cada uno de los 5 usuarios locales configurados, de esta forma cada uno de los ingenieros que realizan el teletrabajo deberán hacer la conexión por medio de los usuarios mediante un cliente VPN, de esta forma son autenticados por el firewall y posteriormente se aplican los respectivos permisos de accesos, establecidos sobre las políticas de firewall.

4.5 ANTECEDENTES

El proyecto aplicado se va a desarrollar al interior de una Pyme enfocada en el sector de tecnologías de la información por lo que se hace necesario realizar una revisión y mejora de la seguridad, por ello durante la ejecución del presente proyecto aplicado se tiene como referencia los siguientes trabajos:

Trabajo de grado para optar por el título de especialista en seguridad Informática de la Universidad Nacional Abierta y a Distancia UNAD titulado “Aplicación de la metodología MAGERIT para el análisis de riesgos de los sistemas de control en la

estación Tenay del oleoducto”[37] cuyo autor es Peña Rojas Hernán Mauricio, en el cual se realiza un análisis de riesgo utilizando los respectivos pasos de la metodología MAGERIT v3 documentados en sus 3 libros, aportando para la elaboración de mi trabajo de grado una guía con la ejecución de un análisis de riesgo detallado, utilizando cada uno de los pasos relacionados en la documentación de MAGERIT.

Trabajo de grado para optar por el título de especialista en seguridad Informática de la Universidad Nacional Abierta y a Distancia UNAD titulado “Análisis de riesgos de los sistemas de seguridad Informática de la empresa KAPPA10 LTDA”[38] cuyo autor es Osorio Briceño Juan Carlos, en el cual se realiza un análisis de riesgo utilizando los la metodología MAGERIT además de ello se ataca mediante una prueba piloto los controles de identidad expuestos en el numeral A11 de la norma ISO 27001 de 2013 Correspondientes a control de acceso, para mitigar las falencias de seguridad relacionadas con la autenticación hacia los firewall Fortigate bajo la administración de la compañía, aportando para la elaboración de mi trabajo de grado la ejecución de un análisis de riesgo basado en MAGERIT, generando el correspondiente levantamiento de activos para un adecuado análisis.

Trabajo de grado para optar por el título de especialista en seguridad Informática de la Universidad Nacional Abierta y a Distancia UNAD titulado “Diseño de seguridad de firewall perimetral para la organización clínica BARRAQUER”[39] cuyo autor es Riveros Leon Paula, en el cual se realiza una implementación de un firewall de seguridad, estableciendo políticas de seguridad con base a las mejores prácticas y estándares internacionales como ISO 27001:2013, aportando en mi trabajo de

[37] ROJAS PEÑA, Hernan. Aplicación de la metodología Magerit para el análisis de riesgos de los sistemas de control en la estación Tenay del Oleoducto Alto Magdalena [en línea]. Disponible en: https://repository.unad.edu.co/handle/10596/27758.
[38] BRICEÑO OSORIO, Juan. Análisis de vulnerabilidades de los sistemas de seguridad informáticos de la empresa Kappa10 LTDA [en línea]. Disponible en: https://repository.unad.edu.co/handle/10596/27822
[39] LEON RIVEROS, Paula. Diseño de seguridad de firewall perimetral para la organización clínica Barraquer. [en línea]. Disponible en: https://repository.unad.edu.co/handle/10596/25634

grado los principios y definiciones de políticas de seguridad sobre Firewall Fortigate de nueva generación, en base al análisis de las necesidades de la compañía según su diseño de red.

5 DISEÑO METODOLÓGICO

5.1 METODOLOGÍA DE INVESTIGACIÓN

El presente proyecto de tipo aplicado nace con el fin de solucionar una problemática identificada en fallas de seguridad informática y seguridad de la información en la empresa B2B TIC SAS. Para ello se requiere la adquisición de competencias como lo detalla Nilda Chávez en su libro:

“El tipo de investigación aplicada tiene como fin principal resolver un problema en un periodo de tiempo corto. Dirigida a la aplicación inmediata mediante acciones concretas para enfrentar el problema. Por tanto, se dirige a la acción inminente y no al desarrollo de la teoría y sus resultados, mediante actividades precisas para enfrentar el problema “[40]

A fin de alcanzar los objetivos definidos para el presente proyecto aplicado se manejan diferentes fases las cuales son:

- Levantamiento de información.

Identificar y definir los distintos componentes de la red actual de la compañía con la ayuda de entrevistas y mediante documentación interna respecto a los distintos activos de la compañía.

- Análisis de información.

Mediante la metodología MAGERIT se realiza la identificación de los activos y su clasificación correspondiente en base a su función, en paralelo se realiza la

[40] CHAVEZ, Nilda. Introducción A La Investigación Educativa.6 ed, Zulia: Editorial La Columna. 2007.

identificación de los requerimientos para la integración del directorio activo y la adición de una segunda capa de seguridad para la autenticación de los usuarios vía VPN.

- Pruebas y puesta en marcha.

En base al análisis e identificación de requerimientos se inician actividades encaminadas a la ejecución de pruebas para confirmar el correcto funcionamiento de la integración del directorio activo y el segundo factor de autenticación para las autenticaciones de los usuarios vía VPN, para finalmente ejecutar la puesta en marcha para todos los usuarios de la compañía B2B TIC SAS.

- Identificación de riesgos y análisis de riesgo.

Se realiza la correspondiente identificación y valoración de las amenazas de los activos para por último determinar el nivel de riesgo.

- Definición de políticas de seguridad en base a resultado de análisis de riesgo.

En base a los resultados del análisis de riesgo se elaboran las respectivas políticas y procedimientos, teniendo como base la norma ISO 27001:2013 en el dominio correspondiente a control de acceso y los objetivos de control:

- Requisitos de negocio para el control de accesos
- Gestión de acceso de usuarios
- Responsabilidades del usuario
- Control de acceso a sistemas y aplicaciones

6 DESARROLLO DE LOS OBJETIVOS

6.1 DESARROLLO DE OBJETIVO 1

- DETERMINAR EL ESTADO ACTUAL DE LA SEGURIDAD INFORMÁTICA DE LA EMPRESA B2B TIC SAS MEDIANTE UN ANÁLISIS DE RIESGOS.

Para el desarrollo del presente objetivo se seleccionó la metodología MAGERIT en su versión 3. Esta es una de las metodologías más reconocidas a nivel mundial, "MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, que estima que la gestión de los riesgos es una piedra angular en las guías de buen gobierno"[41], dispone de amplia documentación apoyada en sus 2 libros y guía técnica, cuenta con detalle y explicación de los pasos para la ejecución de un adecuado análisis de riesgo.

Sin embargo, para el presente proyecto aplicado únicamente se abordarán 3 de los 4 pasos utilizados en la metodología MAGERIT, donde se realiza un proceso de identificación de activos, identificación y valoración de las amenazas de los activos para por ultimo determinar el riesgo, sin llegar a ejecutar el paso cuarto relacionado con la identificación y valoración de salvaguardas ya que el objetivo específico hace referencia a la identificación del estado actual de la seguridad informática de la empresa B2B TIC SAS sin llegar a realizar un tratamiento de los riesgos identificados.

Por medio del levantamiento de información se hace la identificación de los activos de la compañía y de esta manera lograr generar el correspondiente análisis de riesgo.

[41] INCIBE. Principales metodologías de análisis de riesgo utilizadas [En línea]. Disponible en https://www.incibe.es/extfrontinteco/img/File/empresas/dosieres/plan_director_de_seguridad/plan_director_de_seguridad_metodologias_analisis_de_riesgos.pdf

Los activos se clasifican según la metodología MAGERIT en su funcionalidad, la cual se divide en distintos tipos como se registra sobre la Tabla 1.

Tabla 1. Tipos activos información

Tipo de activo	Descripción
Servicios	Servicios activos en los sistemas
Datos/información	archivos, backups, información interna, credenciales, controles de acceso y logs de sistema
Software	Programas, aplicativos, desarrollos, software, sistema de información
Equipos informáticos	hardware, medios materiales, físicos, destinados a soportar los servicios que presta la organización
Personal	Personas relacionadas con los sistemas de información
Redes de comunicaciones	Servicios de comunicaciones contratados a terceros; medios de transporte que llevan datos de un sitio a otro
Soporte de información	Dispositivos físicos que permiten almacenar información de forma permanente
Equipamiento auxiliar	Otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.
Instalaciones	Lugares donde se hospedan los sistemas de información y comunicaciones

Fuente: El Autor

Se llevaron a cabo 2 entrevistas basadas en el formato de entrevistas relacionado sobre el Anexo 3, las cuales se efectuaron telefónicamente, una de ellas realizada al representante legal y la otra al ingeniero de soporte TIC de la compañía.

Como resultado de las entrevistas se obtuvo la relación de activos de la compañía B2B TIC SAS y se procede a realizar la organización según el tipo de activo como se registra en la Tabla 2.

Tabla 2. Activos informáticos B2B TIC SAS

Tipo de Activo	Nombre	Característica
Redes comunicaciones	Ap	Ubiquiti, dedicado servicio inalámbrico
	Modem	Huawei instalado por el proveedor
	Firewall	Fortigate, equipo seguridad
	Switch	Switch HP 1920S 48G

Continuación tabla 2		
Tipo de Activo	**Nombre**	**Característica**
Equipos informáticos	Impresoras escáner	x2 Impresoras HP M681
	UPS	Delta de 20Hw
	Computadores	Portátiles x 10, escritorio x5
	Servidor	x2 Proliant
Soporte de información	Documentos	Archivador para la documentación física
	Página web	Página web en Colombia hosting
Datos información	Archivos información	Se cuenta con un espacio en servidor de archivos y medios extraíbles para el manejo y transporte de información
Personal	Empleados	Actualmente se cuenta con 15 empleados
Software	Sistema operativo	Equipos estandarizados con Windows 10
	Software antivirus	Equipos con Windows defender
	Firewall	Por defecto activo, firewall de Windows.
	Bases de datos	SQL
	ofimática	Office 365
	Correo electrónico	Exchange

Fuente: El Autor

Una vez identificados los activos de la compañía se procedió a generar su tipificación correspondiente con base al libro 2 de la metodología MAGERIT respecto al catálogo de elementos, como se puede observar sobre la Tabla 3.

Tabla 3. Activos informáticos B2B TIC SAS según MAGERIT

Nombre del activo de información	**Proceso propietario del activo**
[HW][mid] Servidor DHCP	Área TIC
[S][dir][idm] Servidor DHCP	Área TIC
[SW][os]Windows 10 pro	Área TIC
[HW][pc] Equipos de Cómputo	Según Asignación
[S][int] Equipos de Cómputo	Área TIC
[HW][]network][firewall] Firewall fortigate	Área TIC
[COM][LAN]Switch HP 1920S	Área TIC
[COM][LAN]ap ubiquiti	Área TIC
[COM][LAN] Firewall fortigate	Área TIC
[D][acl] Firewall fortigate	Área TIC
[S][ipm]Firewall fortigate	Área TIC
[HW]{network}[switch] Switch HP 1920S	Área TIC

Continuación tabla 3	
Nombre del activo de información	**Proceso propietario del activo**
[HW][network][wap] ap ubiquiti	Área TIC
[HW][network][modem] Huawei de ISP	ISP
[COM][LAN]Internet	Área TIC
[HW] Impresoras HP M681	Área TIC
[P][adm] Técnicos TIC	Gestión Humana
[COM][LAN] Puntos de acceso	Área TIC
[AUX][ups] Delta de 20Hw	Área TIC
[SW][std][av]Antivirus	Área TIC
[S] Correo exchange	Área TIC
[S][pub] Página web	COLOMBIAHOSTING/Área TIC
[S][www] Página web	COLOMBIAHOSTING/Área TIC
[SW][sub] Página web	COLOMBIAHOSTING/Área TIC
[D] Página web	COLOMBIAHOSTING/Área TIC
[L][local] oficina TIC	Área TIC
[L][local] Oficina	Gerencia
[SW][office] office 365	Área TIC
[S] Correo exchange	Área TIC
[SW] MySQL 5.7.17	Área TIC
[HW][host] Servidor de archivos	Área TIC
[S][int] Servidor de archivos	Área TIC
[D][files] Servidor de archivos	Área TIC

Fuente: El Autor

Posterior a la normalización de los activos según recomendación de MAGERIT, se identifican las dimensiones de seguridad como lo son disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad las cuales se relacionan en la Tabla 4, adicionalmente se ubican los distintos niveles de valoración y su tipificación dados por la metodología MAGERIT como se observa en la Tabla 5.

Tabla 4. Dimensiones de seguridad en MAGERIT

Dimensión de Seguridad	Nomenclatura	Definición
Disponibilidad	D	Propiedad o característica de los activos consistentes en que las entidades o procesos autorizados tiene acceso a los mismos cuando lo requieren. [UNE 71504:2008]
Integridad	I	Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. [ISO/IEC 13335-1:2004]
Confidencialidad	C	Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. [UNE-ISO/IEC 27001:2007]
Autenticidad	A	Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. [UNE 71504:2008]
Trazabilidad	T	Propiedad o característica consistente en que las actualizaciones de una entidad pueden ser imputadas, exclusivamente a dicha entidad. [UNE 71504:2008]

Fuente: El Autor

Tabla 5. Niveles de valoración activos informáticos MAGERIT

Nivel	Descripción
MA	Muy Alto
A	Alto
M	Medio
B	Bajo
MB	Muy Bajo

Fuente: El Autor

Sobre la Tabla 6 se establece la relevancia de cada activo para la compañía según las dimensiones de disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad dando su correspondiente nivel de valoración.

Tabla 6. Valoración activos según dimensiones

	Dimensiones				
Nombre del activo de información	**Disponibilidad**	**Integridad**	**Confidencialidad**	**Autenticidad**	**Trazabilidad**
[HW][mid] Servidor DHCP	MA	M	M	M	M
[S][dir][idm] Servidor DHCP	MA	M	M	M	M
[SW][os]Windows 10 pro	M	B	B	A	A
[HW][pc] Equipos de Cómputo	A	MA	MA	A	A
[S][int] Equipos de Cómputo	M	B	A	B	M
[HW][]network][firewall] Firewall fortigate	MA	B	B	A	M
[COM][LAN]Switch HP 1920S	MA	M	B	B	B
[COM][LAN]ap ubiquiti	MA	M	B	B	B
[COM][LAN] Firewall fortigate	A	A	A	A	A
[D][acl] Firewall fortigate	MA	A	M	A	A
[S][ipm]Firewall fortigate	A	M	M	A	A
[HW]{network}[switch] Switch HP 1920S	MA	M	B	B	B
[HW][network][wap] ap ubiquiti	A	MA	B	B	M
[HW][network][modem] huawei de ISP	MA	M	B	B	B
[COM][LAN]Internet	MA	M	B	B	M
[HW] Impresoras HP M681	M	M	MA	B	B
[P][adm] Técnicos TIC	MA	MA	MA	B	B
[COM][LAN] Puntos de acceso	MA	M	B	B	B
[AUX][ups] Delta de 20Hw	MA	B	B	B	M
[SW][std][av]Antivirus	MA	A	B	A	M
[S] Correo exchange	A	A	MA	A	B
[S][pub] Página web	A	A	A	A	M
[S][www] Página web	A	A	M	M	M
[SW][sub] Página web	A	A	M	M	M
[D] Página web	MA	MA	MA	MA	MA
[L][local] oficina TIC	A	B	B	B	B
[L][local] Oficina	M	B	B	B	B

Continuación tabla 6					
	Dimensiones				
Nombre del activo de información	**Disponibilidad**	**Integridad**	**Confidencialidad**	**Autenticidad**	**Trazabilidad**
[SW][office] office 365	A	A	M	M	M
[S] Correo exchange	A	A	MA	A	B
[SW] MySQL 5.7.17	MA	A	MA	MA	A
[HW][host] Servidor de archivos	MA	MA	MA	MA	MA
[S][int] Servidor de archivos	MA	MA	M	MA	A
[D][files] Servidor de archivos	MA	MA	A	A	A

Fuente: El Autor

Después de valorar los activos según las dimensiones, se procede a identificar las amenazas de los activos de información. Teniendo en cuenta la clasificación de amenazas de la metodología MAGERIT relacionada en el Anexo 4 en la cual se manejan tipificaciones para amenazas por desastres naturales con la letra N al inicio, industriales letra I al inicio, errores letra E al inicio o ataques con la letra A al inicio como se puede observar en la Tabla 7.

Tabla 7. Identificación de amenazas de los activos de información.

Tipo	Nombre del activo	Amenazas
[HW] Equipamiento informático	[HW][mid] Servidor DHCP	[N1] Fuego
		[N2] Daños por agua
		[N*] Desastres naturales
		[I6] Corte del suministro eléctrico
		[I7] Condiciones inadecuadas de temperatura o humedad
		[E2] Errores del administrador
		[E23] Errores de mantenimiento / actualización de equipos (hardware)
		[E25] Pérdida de equipos
		[A6] Abuso de privilegios de acceso
		[A7] Uso no previsto
		[A11] Acceso no autorizado
[S] Servicios	[S][dir][idm] Servidor DHCP	[E2] Errores del administrador
		[E24] Caída del sistema por agotamiento de recursos
		[A.6] Abuso de privilegios de acceso
		[A.24] Denegación de servicio

Continuación Tabla 7		
Tipo	**Nombre del activo**	**Amenazas**
[SW] software	[SW][os]Windows 10 pro	[E24] Caída del sistema por agotamiento de recursos
		[I.5] Avería de origen físico o lógico
		[E.1] Errores de los usuarios
		[E.2] Errores del administrador
		[E.20] Vulnerabilidades de los programas (software)
		[A.5] Suplantación de la identidad del usuario
		[A.6] Abuso de privilegios de acceso
		[A.7] Uso no previsto
		[A.11] Acceso no autorizado
[HW] Equipamiento informático	[HW][pc] Equipos de Cómputo	[N1] Fuego
		[N2] Daños por agua
		[N*] Desastres naturales
		[I6] Corte del suministro eléctrico
		[I7] Condiciones inadecuadas de temperatura o humedad
		[E2] Errores del administrador
		[E23] Errores de mantenimiento / actualización de equipos (hardware)
		[E25] Pérdida de equipos
		[A6] Abuso de privilegios de acceso
		[A7] Uso no previsto
		[A11] Acceso no autorizado
[S] Servicios	[S][int] Equipos de Cómputo	[A8] Difusión de software dañino
		[A11] Acceso no autorizado
[HW] Equipamiento informático	[HW][]network][firewall] Firewall fortigate	[N1] Fuego
		[N2] Daños por agua
		[N*] Desastres naturales
		[I6] Corte del suministro eléctrico
		[I7] Condiciones inadecuadas de temperatura o humedad
		[E2] Errores del administrador
		[E23] Errores de mantenimiento / actualización de equipos (hardware)
		[E25] Pérdida de equipos
		[A6] Abuso de privilegios de acceso
		[A7] Uso no previsto
		[A11] Acceso no autorizado

Continuación Tabla 7		
Tipo	**Nombre del activo**	**Amenazas**
[COM] Redes de comunicaciones	[COM][LAN]Switch HP 1920S	[I.8] Fallo de servicios de comunicaciones
		[E.2] Errores del administrador
		[A.6] Abuso de privilegios de acceso
		[E.24] Caída del sistema por agotamiento de recursos
		[A.12] Análisis de tráfico
		[A.14] Interceptación de información (escucha)
		[A.24] Denegación de servicio
[COM] Redes de comunicaciones	[COM][LAN]ap ubiquiti	[I.8] Fallo de servicios de comunicaciones
		[E.2] Errores del administrador
		[A.6] Abuso de privilegios de acceso
		[E.24] Caída del sistema por agotamiento de recursos
		[A.12] Análisis de tráfico
		[A.14] Interceptación de información (escucha)
		[A.24] Denegación de servicio
[COM] Redes de comunicaciones	[COM][LAN] Firewall fortigate	[I.8] Fallo de servicios de comunicaciones
		[E.2] Errores del administrador
		[A.6] Abuso de privilegios de acceso
		[E.24] Caída del sistema por agotamiento de recursos
		[A.12] Análisis de tráfico
		[A.14] Interceptación de información (escucha)
		[A.24] Denegación de servicio
[D] Datos	[D][acl] Firewall fortigate	[E.2] Errores del administrador
		[E.19] Fugas de información
		[A.6] Abuso de privilegios de acceso
		[A.11] Acceso no autorizado
		[A.19] Divulgación de información
[S] Servicios	[S][ipm]Firewall fortigate	[A11] Acceso no autorizado
		[E.2] Errores del administrador
		[E.9] Errores de [re-]encaminamiento
		[E.24] Caída del sistema por agotamiento de recursos
		[A.24] Denegación de servicio

Continuación Tabla 7		
Tipo	**Nombre del activo**	**Amenazas**
[HW] Equipamiento informático	[HW]{network}[switch] Switch HP 1920S	[N1] Fuego
		[N2] Daños por agua
		[N*] Desastres naturales
		[I6] Corte del suministro eléctrico
		[I7] Condiciones inadecuadas de temperatura o humedad
		[E2] Errores del administrador
		[E23] Errores de mantenimiento / actualización de equipos (hardware)
		[E25] Pérdida de equipos
		[A6] Abuso de privilegios de acceso
		[A7] Uso no previsto
		[A11] Acceso no autorizado
[HW] Equipamiento informático	[HW][network][wap] ap ubiquiti	[N1] Fuego
		[N2] Daños por agua
		[N*] Desastres naturales
		[I6] Corte del suministro eléctrico
		[I7] Condiciones inadecuadas de temperatura o humedad
		[E2] Errores del administrador
		[E23] Errores de mantenimiento / actualización de equipos (hardware)
		[E25] Pérdida de equipos
		[A6] Abuso de privilegios de acceso
		[A7] Uso no previsto
		[A11] Acceso no autorizado
[HW] Equipamiento informático	[HW][network][modem] huawei de ISP	[N1] Fuego
		[N2] Daños por agua
		[N*] Desastres naturales
		[I6] Corte del suministro eléctrico
		[I7] Condiciones inadecuadas de temperatura o humedad
		[E2] Errores del administrador
		[E23] Errores de mantenimiento / actualización de equipos (hardware)
		[E25] Pérdida de equipos
		[A6] Abuso de privilegios de acceso
		[A11] Acceso no autorizado

Continuación Tabla 7		
Tipo	**Nombre del activo**	**Amenazas**
[COM] Redes de comunicaciones	[COM][LAN]Internet	[I.8] Fallo de servicios de comunicaciones
		[E.2] Errores del administrador
		[E.24] Caída del sistema por agotamiento de recursos
		[A.12] Análisis de tráfico
		[A.14] Interceptación de información (escucha)
		[A.24] Denegación de servicio
[HW] Equipamiento informático	[HW] Impresoras HP M681	[N1] Fuego
		[N2] Daños por agua
		[N*] Desastres naturales
		[I6] Corte del suministro eléctrico
		[I7] Condiciones inadecuadas de temperatura o humedad
		[E2] Errores del administrador
		[E23] Errores de mantenimiento / actualización de equipos (hardware)
		[E25] Pérdida de equipos
[P] Personal	[P][adm] Técnicos TIC	[A30] Ingeniería social (picaresca)
		[E.19] Fugas de información
		[E.28] Indisponibilidad del personal
[COM] Redes de comunicaciones	[COM][LAN] Puntos de acceso	[E.2] Errores del administrador
		[E.24] Caída del sistema por agotamiento de recursos
		[A.12] Análisis de tráfico
		[A.14] Interceptación de información (escucha)
[AUX] Equipamiento auxiliar	[AUX][ups] Delta de 20Hw	[N.1] Fuego
		[N.2] Daños por agua
		[N.*] Desastres naturales
		[I.5] Avería de origen físico o lógico
		[I.7] Condiciones inadecuadas de temperatura o humedad
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)

Continuación Tabla 7		
Tipo	**Nombre del activo**	**Amenazas**
[SW] Software	[SW][std][av]Antivirus	[E24] Caída del sistema por agotamiento de recursos
		[E.1] Errores de los usuarios
		[E.2] Errores del administrador
		[E.20] Vulnerabilidades de los programas (software)
		[E.21] Errores de mantenimiento / actualización de programas (software)
		[A.8] Difusión de software dañino
		[A.19] Divulgación de información
		[A.22] Manipulación de programas
[S] Servicios	[S] Correo exchange	[E.1] Errores de los usuarios
		[E.2] Errores del administrador
		[E.19] Fugas de información
		[E.24] Caída del sistema por agotamiento de recursos
		[A.5] Suplantación de la identidad del usuario
		[A.24] Denegación de servicio
[S] Servicios	[S][pub] Página web/[S][www] Página web	[E.1] Errores de los usuarios
		[E.2] Errores del administrador
		[E.19] Fugas de información
		[E.24] Caída del sistema por agotamiento de recursos
		[A.5] Suplantación de la identidad del usuario
		[A.24] Denegación de servicio
[SW] Software	[SW][sub] Página web	[E24] Caída del sistema por agotamiento de recursos
		[E.2] Errores del administrador
		[E.20] Vulnerabilidades de los programas (software)
		[E.21] Errores de mantenimiento / actualización de programas (software)
		[A.8] Difusión de software dañino
[D] Datos	[D] Página web	[E1] Errores de los usuarios
		[E15] Alteración accidental de la información
		[E19] Fugas de información
		[A6] Abuso de privilegios de acceso
		[A11] Acceso no autorizado
		[A15] Modificación deliberada de la información

Continuación Tabla 7		
Tipo	**Nombre del activo**	**Amenazas**
[L] Instalaciones	[L][local] oficina TIC/[L][local] Oficina	[N1] Fuego
		[N2] Daños por agua
		[N*] Desastres naturales
		[E18] Destrucción de información
		[E19] Fugas de información
		[A11] Acceso no autorizado
		[A18] Destrucción de información
		[E19] Fugas de información
		[A26] Ataque destructivo
		[A27] Ocupación enemiga
[SW] Software	[SW][office] office 365	[A14] Interceptación de información (escucha)
		[E24] Caída del sistema por agotamiento de recursos
[S] Servicios	[S] Correo exchange	[E2] Errores del administrador
		[A11] Acceso no autorizado
		[A.5] Suplantación de la identidad del usuario
		[A.24] Denegación de servicio
[SW] Software	[SW] MySQL 5.7.17	[E24] Caída del sistema por agotamiento de recursos
		[E.1] Errores de los usuarios
		[A.19] Divulgación de información
		[A.22] Manipulación de programas
		[E.2] Errores del administrador
		[E.20] Vulnerabilidades de los programas (software)
		[E.21] Errores de mantenimiento / actualización de programas (software)
[HW] Equipamiento informático	[HW][host] Servidor de archivos	[N1] Fuego
		[N2] Daños por agua
		[N*] Desastres naturales
		[I6] Corte del suministro eléctrico
		[I7] Condiciones inadecuadas de temperatura o humedad
		[E2] Errores del administrador
		[E23] Errores de mantenimiento / actualización de equipos (hardware)
		[E25] Pérdida de equipos
		[A6] Abuso de privilegios de acceso
		[A7] Uso no previsto
		[A11] Acceso no autorizado

Continuación Tabla 7		
Tipo	**Nombre del activo**	**Amenazas**
[S] Servicios	[S][int] Servidor de archivos	[E.1] Errores de los usuarios
		[E.2] Errores del administrador
		[E.19] Fugas de información
		[E.24] Caída del sistema por agotamiento de recursos
		[A.5] Suplantación de la identidad del usuario
		[A.24] Denegación de servicio
[D] Datos	[D][files] Servidor de archivos	[E14] Escapes de información
		[E1] Errores de los usuarios
		[E15] Alteración accidental de la información
		[E19] Fugas de información
		[A6] Abuso de privilegios de acceso
		[A11] Acceso no autorizado
		[A15] Modificación deliberada de la información

Fuente: El Autor

A continuación, se realiza la identificación de vulnerabilidades y riesgo, se genera la respectiva evaluación del riesgo teniendo en cuenta los valores de impacto que van desde MB muy bajo a MA muy alto los cuales determinan el daño que puede ocasionar la materialización de una amenaza a un activo, esta valoración se detalla sobre la Tabla 8 y sobre la Tabla 9 se muestra la valoración de la probabilidad la cual corresponde a la posibilidad de que una amenaza se materialice.

Tabla 8. Valores de impacto en el riesgo

IMPACTO		
Nomenclatura	**categoría**	**valoración**
MA	Muy Alto	5
A	Alto	4
M	Medio	3
B	Bajo	2
MB	Muy Bajo	1

Fuente: El Autor

Tabla 9. Valores probabilidad ocurrencia del riesgo

	PROBABILIDAD DEL RIESGO		
	Nomenclatura	**categoría**	**valoración**
Probabilidad	MA	Prácticamente seguro	5
	A	Probable	4
	M	Posible	3
	B	Poco probable	2
	MB	Muy raro	1

Fuente: El Autor

Para poder determinar la valoración del riesgo que recae en un activo se utiliza la Tabla 10 sobre la cual se observa en los ejes X-Y impacto y probabilidad evidenciando su relación al aplicar la fórmula riesgo= probabilidad * impacto. El resultado de la aplicación de la fórmula es un valor numérico en el rango de 1 a 25 para de esta forma realizar su categorización como se observa en la Tabla 11, con ello se procede a valorar el riesgo sobre los activos de la compañía como se observa en la Tabla 12, en la cual se relacionan activos, amenazas, riesgos, vulnerabilidades y se calcula la valoración del riesgo con base a probabilidad e impacto.

Tabla 10. Tabla fórmula del riesgo

IMPACTO	**MA**	5	10	15	20	25
	A	4	8	12	16	20
	M	3	6	9	12	15
	B	2	4	6	8	10
	MB	1	2	3	4	5
RIESGO		**MB**	**B**	**M**	**A**	**MA**
		PROBABILIDAD				

Fuente: El Autor

Tabla 11. Valoración del riesgo

VALORACIÓN DEL RIESGO			
	Nomenclatura	**categoría**	**valoración**
valoración del riesgo	MA	**Critico**	21 a 25
	A	**Importante**	16 a 20
	M	**Apreciable**	10 a 15
	B	**Bajo**	5 a 9
	MB	**Despreciable**	1 a 4

Fuente: El Autor

Tabla 12. Valoración de riesgo sobre activos

				Valoración del Riesgo			
Nombre del activo	**Vulnerabilidad**	**Amenazas**	**Riesgo**	**Probabilidad**	**Impacto**	**valoración**	**Nivel de Riesgo**
[HW][mid] Servidor DHCP	La ubicación no cuenta con los elementos necesarios para el control de temperatura y humedad necesarios	[I.7] Condiciones inadecuadas de temperatura o humedad	Daño, reducción tiempo vida	3	4	12	M
	No se evidencia la existencia de manuales de procedimientos que permitan realizar las actividades de administración de forma estándar y controlada	[E.2] Errores del administrador	caída o indisponibilidad	3	5	15	M
	No se evidencia la presencia de planes de mantenimiento preventivo y correctivo y la existencia de manuales de procedimientos que permitan realizar las actividades de administración de forma estándar y controlada	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	caída, mal funcionamiento o indisponibilidad	4	5	20	A
	No se evidencia la existencia de controles de acceso al recurso	[E.25] Pérdida de equipos	Indisponibilidad, robo	2	5	10	M
	No se evidencia esquema de privilegios individualizados por los roles de los usuarios	[A.6] Abuso de privilegios de acceso	Robo, perdida de confidencialidad	4	4	16	A
	Planes de monitoreo de los recursos del servidor escasos	[A.7] Uso no previsto	Ineficiencia en el uso de los recursos	3	4	12	M
	Falta de controles de seguridad para el acceso al servidor	[A.11] Acceso no autorizado	Robo, perdida o adulteración de información	4	5	20	A
[S][dir][idm] Servidor DHCP	No se evidencia la existencia de manuales de procedimientos que permitan realizar las actividades de administración de forma estándar y controlada	[E.2] Errores del administrador	caída o indisponibilidad	3	5	15	M
	No se cuenta con rangos específicos para la asignación de DHCP	[E.24] Caída del sistema por agotamiento de recursos	caída o indisponibilidad	3	5	15	M
[SW][os]Windows 10 pro	No se cuenta con tareas de mantenimiento preventivo y o actualización de parches	[E.24] Caída del sistema por agotamiento de recursos	caída o indisponibilidad	4	2	8	B
	No se evidencia la existencia de manuales de procedimientos que permitan realizar las actividades de administración de forma estándar y controlada	[E.2] Errores del administrador	caída o indisponibilidad	3	2	6	B
	No se cuenta con tareas de mantenimiento preventivo	[E.20] Vulnerabilidades de los programas (software)	Falla en la confidencialidad e integridad	4	4	16	A
	No se cuenta con registro de actividades de usuario y manejo de software	[A.7] Uso no previsto	perdida de confidencialidad, disponibilidad	3	3	9	B
	Falta de controles de seguridad para el acceso y monitoreo	[A.11] Acceso no autorizado	Robo, perdida o adulteración de información	3	4	12	M

Continuación Tabla 12							
Nombre del activo	**Vulnerabilidad**	**Amenazas**	**Riesgo**	**Probabilidad**	**Impacto**	**valoración**	**Nivel de Riesgo**
[HW][pc] Equipos de Cómputo	No se evidencia la existencia de manuales de procedimientos que permitan realizar las actividades de administración de forma estándar y controlada	[E.2] Errores del administrador	caída o indisponibilidad	3	3	9	B
	No se evidencia la presencia de planes de mantenimiento preventivo y correctivo y la existencia de manuales de procedimientos que permitan realizar las actividades de administración de forma estándar y controlada	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	caída, mal funcionamiento o indisponibilidad	3	4	12	M
	No se cuenta con guayas de seguridad	[E.25] Pérdida de equipos	Indisponibilidad, robo	4	5	20	A
	No se cuenta con registro de actividades de usuario y manejo de software	[A.7] Uso no previsto	Perdida de confidencialidad, disponibilidad	4	4	16	A
	Falta de controles de seguridad para el acceso y monitoreo	[A.11] Acceso no autorizado	Robo, perdida o adulteración de información	3	4	12	M
[S][int] Equipos de Cómputo	No se cuenta con seguimiento a nivel de endpoint para detectar comportamientos anómalos	[A.8] Difusión de software dañino	Perdida de confidencialidad, robo o secuestro	3	4	12	M
	Falta de controles de seguridad para el acceso y monitoreo	[A.11] Acceso no autorizado	Robo, perdida o adulteración de información	3	4	12	M
[HW][]network][firewall] Firewall fortigate	La ubicación no cuenta con los elementos necesarios para el control de temperatura y humedad necesarios	[I.7] Condiciones inadecuadas de temperatura o humedad	Daño, reducción tiempo vida	3	5	15	M
	No se evidencia la existencia de manuales de procedimientos que permitan realizar las actividades de administración de forma estándar y controlada	[E.2] Errores del administrador	Caída o indisponibilidad	4	5	20	A
	No se evidencia la presencia de planes de mantenimiento preventivo y correctivo y la existencia de manuales de procedimientos que permitan realizar las actividades de administración de forma estándar y controlada	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Caída, mal funcionamiento o indisponibilidad	4	5	20	A
	No se evidencia la existencia de controles de acceso al recurso	[E.25] Pérdida de equipos	Indisponibilidad, robo	2	5	10	M
	Falta de controles de seguridad para el acceso	[A.11] Acceso no autorizado	Robo, perdida o adulteración de información	3	5	15	M

Continuación Tabla 12							
Nombre del activo	**Vulnerabilidad**	**Amenazas**	**Riesgo**	**Probabilidad**	**Impacto**	**valoración**	**Nivel de Riesgo**
[COM][LAN]Switch HP 1920S	No se cuenta con herramientas de monitoreo que registren estado	[I.8] Fallo de servicios de comunicaciones	Perdida de conectividad LAN	4	5	20	A
	No se evidencia la existencia de manuales de procedimientos que permitan realizar las actividades de administración de forma estándar y controlada	[E.2] Errores del administrador	Caída o indisponibilidad	3	5	15	M
	No se cuenta con control de ancho de banda o monitoreo de red para detectar comportamientos anómalos	[E.24] Caída del sistema por agotamiento de recursos	Caída, intermitencia o lentitud	4	5	20	A
	No se cuenta con gestión de cambios y o seguimiento de estado de la red	[A.12] Análisis de tráfico	Perdida de confidencialidad	3	4	12	M
	No se cuenta con protección de Dos	[A.24] Denegación de servicio	Caída o indisponibilidad	3	5	15	M
[COM][LAN]ap ubiquiti	No se cuenta con herramientas de monitoreo que registren estado	[I.8] Fallo de servicios de comunicaciones	Perdida de conectividad LAN	3	2	6	B
	No se evidencia la existencia de manuales de procedimientos que permitan realizar las actividades de administración de forma estándar y controlada	[E.2] Errores del administrador	Caída o indisponibilidad	3	2	6	B
	No se cuenta con control de ancho de banda o monitoreo de red para detectar comportamientos anómalos	[E.24] Caída del sistema por agotamiento de recursos	caída, intermitencia o lentitud	3	3	9	B
	no se cuenta con gestión de cambios y o seguimiento de estado de la red	[A.12] Análisis de tráfico	Perdida de confidencialidad	3	3	9	B
	Falta monitoreo de la red, políticas y segmentación adecuada	[A.14] Interceptación de información (escucha)	Perdida de confidencialidad	3	4	12	M
	No se cuenta con protección de Dos	[A.24] Denegación de servicio	Caída o indisponibilidad	4	3	12	M
[COM][LAN] Firewall fortigate	No se cuenta con herramientas de monitoreo que registren estado	[I.8] Fallo de servicios de comunicaciones	Perdida de conectividad LAN/WAN	5	5	25	MA
	No se evidencia la existencia de manuales de procedimientos que permitan realizar las actividades de administración de forma estándar y controlada	[E.2] Errores del administrador	Caída o indisponibilidad	3	5	15	M
	No se cuenta con control de ancho de banda o monitoreo de red para detectar comportamientos anómalos	[E.24] Caída del sistema por agotamiento de recursos	Caída, intermitencia o lentitud	3	5	15	M
	no se cuenta con gestión de cambios y o seguimiento de estado de la red	[A.12] Análisis de tráfico	Perdida de confidencialidad	2	4	8	B
	Falta monitoreo de la red, políticas y segmentación adecuada	[A.14] Interceptación de información (escucha)	Perdida de confidencialidad	3	4	12	M
	No se cuenta con políticas de protección de Dos	[A.24] Denegación de servicio	Caída o indisponibilidad	4	5	20	A

Continuación Tabla 12							
Nombre del activo	**Vulnerabilidad**	**Amenazas**	**Riesgo**	**Probabilidad**	**Impacto**	**valoración**	**Nivel de Riesgo**
[D][acl] Firewall fortigate	No se evidencia la existencia de manuales de procedimientos que permitan realizar las actividades de administración de forma estándar y controlada	[E.2] Errores del administrador	Caída o indisponibilidad	3	4	12	M
	No se cuenta con monitoreo y o seguimiento a actividad de usuarios	[A.6] Abuso de privilegios de acceso	Falla en la confidencialidad e integridad	4	5	20	A
	Falta de controles de seguridad para el acceso	[A.11] Acceso no autorizado	Robo, perdida o adulteración de información	4	5	20	A
[S][ipm]Firewall fortigate	Falta de controles de seguridad para el acceso	[A.11] Acceso no autorizado	Robo, perdida o adulteración de información	4	5	20	A
	No se evidencia la existencia de manuales de procedimientos que permitan realizar las actividades de administración de forma estándar y controlada	[E.2] Errores del administrador	Caída o indisponibilidad	4	5	20	A
	No se cuenta con control de cambios o monitoreo de actividades de configuración	[E.9] Errores de [re-]encaminamiento	Indisponibilidad o perdida de confidencialidad.	2	5	10	M
	No se cuenta con control de ancho de banda o monitoreo de red para detectar comportamientos anómalos	[E.24] Caída del sistema por agotamiento de recursos	Caída, intermitencia o lentitud	5	5	25	MA
	No se cuenta con políticas de protección de Dos	[A.24] Denegación de servicio	Caída o indisponibilidad	4	5	20	A
[HW]{network}[switch] Switch HP 1920S	La ubicación no cuenta con los elementos necesarios para el control de temperatura y humedad necesarios	[I.7] Condiciones inadecuadas de temperatura o humedad	Daño, reducción tiempo vida	2	4	8	B
	No se evidencia la existencia de manuales de procedimientos que permitan realizar las actividades de administración de forma estándar y controlada	[E.2] Errores del administrador	Caída o indisponibilidad	3	4	12	M
	No se evidencia la presencia de planes de mantenimiento preventivo y correctivo y la existencia de manuales de procedimientos que permitan realizar las actividades de administración de forma estándar y controlada	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Caída, mal funcionamiento o indisponibilidad	3	4	12	M
	No se evidencia la existencia de controles de acceso al recurso	[E.25] Pérdida de equipos	Indisponibilidad, robo	2	4	8	B
	No se cuenta con monitoreo y o seguimiento a actividad de usuarios	[A.6] Abuso de privilegios de acceso	Falla en la confidencialidad e integridad	3	4	12	M
	Falta de controles de seguridad para el acceso	[A.11] Acceso no autorizado	Robo, perdida o adulteración de información	3	4	12	M

Continuación Tabla 12							
Nombre del activo	**Vulnerabilidad**	**Amenazas**	**Riesgo**	**Probabilidad**	**Impacto**	**valoración**	**Nivel de Riesgo**
[HW][network][wap] ap ubiquiti	La ubicación no cuenta con los elementos necesarios para el control de temperatura y humedad necesarios	[I.7] Condiciones inadecuadas de temperatura o humedad	Daño, reducción tiempo vida	3	3	9	B
	No se evidencia la existencia de manuales de procedimientos que permitan realizar las actividades de administración de forma estándar y controlada	[E.2] Errores del administrador	Caída o indisponibilidad	3	2	6	B
	No se evidencia la presencia de planes de mantenimiento preventivo y correctivo y la existencia de manuales de procedimientos que permitan realizar las actividades de administración de forma estándar y controlada	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Caída, mal funcionamiento o indisponibilidad	3	2	6	B
	No se evidencia la existencia de controles de acceso al recurso	[E.25] Pérdida de equipos	Indisponibilidad, robo	2	3	6	B
	Falta de controles de seguridad para el acceso	[A.11] Acceso no autorizado	Robo, perdida o adulteración de información	3	4	12	M
[HW][network][modem] huawei de ISP	La ubicación no cuenta con los elementos necesarios para el control de temperatura y humedad necesarios	[I.7] Condiciones inadecuadas de temperatura o humedad	Daño, reducción tiempo vida	3	5	15	M
	No se evidencia la existencia de manuales de procedimientos que permitan realizar las actividades de administración de forma estándar y controlada	[E.2] Errores del administrador	Caída o indisponibilidad	3	5	15	M
	No se evidencia la presencia de planes de mantenimiento preventivo y correctivo y la existencia de manuales de procedimientos que permitan realizar las actividades de administración de forma estándar y controlada	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Caída, mal funcionamiento o indisponibilidad	4	5	20	A
	No se evidencia la existencia de controles de acceso al recurso	[E.25] Pérdida de equipos	Indisponibilidad, robo	2	5	10	M
	Falta de controles de seguridad para el acceso	[A.11] Acceso no autorizado	Robo, perdida o adulteración de información	3	5	15	M
[COM][LAN]Internet	No se cuenta con herramientas de monitoreo que registren estado	[I.8] Fallo de servicios de comunicaciones	Perdida de conectividad WAN	5	5	25	MA
	No se evidencia la existencia de manuales de procedimientos que permitan realizar las actividades de administración de forma estándar y controlada	[E.2] Errores del administrador	Caída o indisponibilidad	4	5	20	A
	No se cuenta con control de ancho de banda o monitoreo de red para detectar comportamientos anómalos	[E.24] Caída del sistema por agotamiento de recursos	Caída, intermitencia o lentitud	5	5	25	MA
	No se cuenta con protección de Dos	[A.24] Denegación de servicio	Caída o indisponibilidad	4	5	20	A

Continuación Tabla 12							
Nombre del activo	**Vulnerabilidad**	**Amenazas**	**Riesgo**	**Probabilidad**	**Impacto**	**valoración**	**Nivel de Riesgo**
[HW] Impresoras HP M681	La ubicación no cuenta con los elementos necesarios para el control de temperatura y humedad necesarios	[I.7] Condiciones inadecuadas de temperatura o humedad	Daño, reducción tiempo vida	2	3	6	B
	No se evidencia la existencia de manuales de procedimientos que permitan realizar las actividades de administración de forma estándar y controlada	[E.2] Errores del administrador	Caída o indisponibilidad	2	3	6	B
	No se evidencia la presencia de planes de mantenimiento preventivo y correctivo y la existencia de manuales de procedimientos que permitan realizar las actividades de administración de forma estándar y controlada	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Caída, mal funcionamiento o indisponibilidad	3	3	9	B
	No se cuenta con guayas de seguridad	[E.25] Pérdida de equipos	Indisponibilidad, robo	2	4	8	B
[P][adm] Técnicos TIC	Pendiente planes de capacitación temas seguridad informática	[A,30] Ingeniería social (picaresca)	Falla en la confidencialidad e integridad	4	5	20	A
	No se evidencia la existencia de programas de formación y culturización en seguridad informática	[E.19] Fugas de información	Falla en la confidencialidad e integridad	4	5	20	A
	No se cuenta con adecuado entrenamiento o personal con rol de backup	[E.28] Indisponibilidad del personal	Indisponibilidad de atención o demoras que perjudiquen la operación	5	4	20	A
[COM][LAN] Puntos de acceso	No se evidencia la existencia de manuales de procedimientos que permitan realizar las actividades de administración de forma estándar y controlada	[E.2] Errores del administrador	Caída o indisponibilidad	3	3	9	B
	No se cuenta con control de ancho de banda o monitoreo de red para detectar comportamientos anómalos	[E.24] Caída del sistema por agotamiento de recursos	Caída, intermitencia o lentitud	3	3	9	B
	Falta monitoreo de la red, políticas y segmentación adecuada	[A.14] Interceptación de información (escucha)	Perdida de confidencialidad	3	3	9	B
[AUX][ups] Delta de 20Hw	No se cuenta con tareas de mantenimiento preventivo	[I.5] Avería de origen físico o lógico	Daño	4	5	20	A
	La ubicación no cuenta con los elementos necesarios para el control de temperatura y humedad necesarios	[I.7] Condiciones inadecuadas de temperatura o humedad	Daño, reducción tiempo vida	3	4	12	M
	No se evidencia la presencia de planes de mantenimiento preventivo y correctivo y la existencia de manuales de procedimientos que permitan realizar las actividades de administración de forma estándar y controlada	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Caída, mal funcionamiento o indisponibilidad	4	4	16	A

Continuación Tabla 12							
Nombre del activo	**Vulnerabilidad**	**Amenazas**	**Riesgo**	**Probabilidad**	**Impacto**	**valoración**	**Nivel de Riesgo**
[SW][std][av]Antivirus	No se cuenta con monitoreo de estado de bases de datos de antivirus o actividad	[E.24] Caída del sistema por agotamiento de recursos	Caída, intermitencia o lentitud	3	3	9	B
	No se evidencia proceso de control y seguimiento de registros para validar que la actividad	[E.1] Errores de los usuarios	Fallas en la confidencialidad y robo	3	3	9	B
	No se evidencia la existencia de manuales de procedimientos que permitan realizar las actividades de administración de forma estándar y controlada	[E.2] Errores del administrador	Caída o indisponibilidad	3	3	9	B
	No se cuenta con tareas de mantenimiento preventivo	[E.20] Vulnerabilidades de los programas (software)	Falla en la confidencialidad e integridad	4	4	16	A
	No se evidencia la presencia de planes de mantenimiento preventivo y correctivo y la existencia de manuales de procedimientos que permitan realizar las actividades de administración de forma estándar y controlada	[E.21] Errores de mantenimiento / actualización de programas (software)	perdida de integridad, disponibilidad.	3	3	9	B
	No se cuenta con monitoreo de estado de bases de datos de antivirus	[A.8] Difusión de software dañino	Perdida de confidencialidad, robo o secuestro	3	4	12	M
	Falta monitoreo y validación estado de antivirus	[A.19] Divulgación de información	Robo, perdida confidencialidad	4	5	20	A
[S] Correo exchange	No se evidencia proceso de control y seguimiento de registros para validar que la información registrada por los usuarios no violenta los acuerdos de privacidad y confidencialidad	[E.1] Errores de los usuarios	Fallas en la confidencialidad y robo	3	3	9	B
	No se evidencia la existencia de manuales de procedimientos que permitan realizar las actividades de administración de forma estándar y controlada	[E.2] Errores del administrador	Caída o indisponibilidad	3	4	12	M
	No se evidencia la existencia de programas de formación y culturización en seguridad informática	[E.19] Fugas de información	Falla en la confidencialidad e integridad	4	5	20	A
	Inadecuado manejo de servicios generados por múltiples tareas y o conexiones	[E.24] Caída del sistema por agotamiento de recursos	Caída, intermitencia o lentitud	4	5	20	A
	No se cuenta con monitoreo y o seguimiento a actividad de usuarios	[A.5] Suplantación de la identidad del usuario	Falla en la confidencialidad e integridad	4	5	20	A
	Se desconoce información de plan y anti Dos	[A.24] Denegación de servicio	Caída o indisponibilidad	3	4	12	M

Continuación Tabla 12							
Nombre del activo	**Vulnerabilidad**	**Amenazas**	**Riesgo**	**Probabilidad**	**Impacto**	**valoración**	**Nivel de Riesgo**
[S][pub] Página web/[S][www] Página web	No se evidencia proceso de control y seguimiento de registros para validar que la información registrada por los usuarios no violenta los acuerdos de privacidad y confidencialidad	[E.1] Errores de los usuarios	Fallas en la confidencialidad y robo	4	4	16	A
	No se evidencia la existencia de manuales de procedimientos que permitan realizar las actividades de administración de forma estándar y controlada	[E.2] Errores del administrador	Caída o indisponibilidad	3	5	15	M
	No se evidencia la existencia de programas de formación y culturización en seguridad informática	[E.19] Fugas de información	Falla en la confidencialidad e integridad	4	5	20	A
	No se cuenta con conocimiento de capacidades del hosting	[E.24] Caída del sistema por agotamiento de recursos	caída, intermitencia o lentitud	4	5	20	A
	No se cuenta con monitoreo y o seguimiento a actividad de usuarios	[A.5] Suplantación de la identidad del usuario	Falla en la confidencialidad e integridad	3	4	12	M
	No se cuenta con protección de Dos	[A.24] Denegación de servicio	caída o indisponibilidad	4	5	20	A
[SW][sub] Página web	No se cuenta con conocimiento de capacidades del hosting	[E.24] Caída del sistema por agotamiento de recursos	Caída, intermitencia o lentitud	4	5	20	A
	No se evidencia la existencia de manuales de procedimientos que permitan realizar las actividades de administración de forma estándar y controlada	[E.2] Errores del administrador	Caída o indisponibilidad	4	5	20	A
	No se cuenta con tareas de análisis de vulnerabilidades	[E.20] Vulnerabilidades de los programas (software)	Falla en la confidencialidad e integridad	4	5	20	A
	No se evidencia la presencia de planes de mantenimiento preventivo y correctivo y la existencia de manuales de procedimientos que permitan realizar las actividades de administración de forma estándar y controlada	[E.21] Errores de mantenimiento / actualización de programas (software)	indisponibilidad - lentitud	4	5	20	A
[D] Página web	No se cuenta con control de cambios o monitoreo de actividades de configuración	[E,15] Alteración accidental de la información	Indisponibilidad o perdida de confidencialidad.	5	5	25	MA
	No se tiene trazabilidad de la información alojada ni seguimiento a actividad	[E.19] Fugas de información	Falla en la confidencialidad e integridad	4	5	20	A
	No se cuenta con monitoreo y o seguimiento a actividad de usuarios	[A.6] Abuso de privilegios de acceso	Falla en la confidencialidad e integridad	4	5	20	A
	Falta de controles de acceso mediante segunda capa de autenticación	[A.11] Acceso no autorizado	Robo, perdida o adulteración de información	4	5	20	A
	No se cuenta con control de cambios o inventario de información	[A15] Modificación deliberada de la información	perdida de integridad o robo	4	5	20	A

Continuación Tabla 12							
Nombre del activo	**Vulnerabilidad**	**Amenazas**	**Riesgo**	**Probabilidad**	**Impacto**	**valoración**	**Nivel de Riesgo**
[L][local] oficina TIC/[L][local] Oficina	La ubicación del recurso no cuenta con sistema de control de incendios	[N.1] Fuego	Perdida - daño del equipo.	2	5	10	M
	La ubicación del recurso no cuenta con sistema de control de inundaciones	[N.2] Daños por agua	Perdida - daño del equipo.	2	5	10	M
	La ubicación no cuenta con las características de protección frente a catástrofes naturales	[N.*] Desastres naturales	Perdida - daño del equipo.	3	5	15	M
	No se cuenta con adecuado almacenamiento y destrucción de documentación	[E,18] Destrucción de información	Perdida de confidencialidad e integridad.	3	5	15	M
	No se cuenta con condiciones para almacenamiento de documentación sensible	[E.19] Fugas de información	Falla en la confidencialidad e integridad	3	4	12	M
	Falta de controles de seguridad para el acceso	[A.11] Acceso no autorizado	Robo, perdida o adulteración de información	3	5	15	M
	No se cuenta con controles de acceso adecuados para las oficinas y falta adecuado registro de ingresos	[A.18] Destrucción de información	Robo, perdida	3	4	12	M
	No se cuenta con condiciones para almacenamiento de documentación sensible	[E.19] Fugas de información	Falla en la confidencialidad e integridad	3	4	12	M
	ubicación a vías principales pueden generar vandalismo o terrorismo	[A26] Ataque destructivo	Robo, perdida	2	4	8	B
	ubicación a vías principales pueden generar vandalismo o terrorismo	[A27] Ocupación enemiga	Robo, indisponibilidad, perdida de confidencialidad	2	4	8	B
[SW][office] office 365	No se cuenta con conocimiento de capacidades servicio contratado	[E.24] Caída del sistema por agotamiento de recursos	Caída, intermitencia o lentitud	3	4	12	M
[S] Correo exchange	No se evidencia la existencia de manuales de procedimientos que permitan realizar las actividades de administración de forma estándar y controlada	[E.2] Errores del administrador	Caída o indisponibilidad	2	4	8	B
	Falta de controles de acceso mediante segunda capa de autenticación	[A.11] Acceso no autorizado	Robo, perdida o adulteración de información	3	4	12	M
	No se cuenta con monitoreo y o seguimiento a actividad de usuarios	[A.5] Suplantación de la identidad del usuario	Falla en la confidencialidad e integridad	4	5	20	A

Continuación Tabla 12							
Nombre del activo	**Vulnerabilidad**	**Amenazas**	**Riesgo**	**Probabilidad**	**Impacto**	**valoración**	**Nivel de Riesgo**
[SW] MySQL 5.7.17	No se cuenta con monitoreo de recursos o manejo de alertas	[E.24] Caída del sistema por agotamiento de recursos	Caída, intermitencia o lentitud	4	5	20	A
	No se evidencia proceso de control y seguimiento de registros para validar que la información registrada por los usuarios no violenta los acuerdos de privacidad y confidencialidad	[E.1] Errores de los usuarios	Fallas en la confidencialidad y robo	3	4	12	M
	Falta monitoreo y validación estado de antivirus	[A.19] Divulgación de información	Robo, perdida confidencialidad	4	5	20	A
	No se evidencia la existencia de manuales de procedimientos que permitan realizar las actividades de administración de forma estándar y controlada	[E.2] Errores del administrador	Caída o indisponibilidad	4	5	20	A
	No se cuenta con tareas de mantenimiento preventivo	[E.20] Vulnerabilidades de los programas (software)	Falla en la confidencialidad e integridad	5	5	25	MA
	No se evidencia la presencia de planes de mantenimiento preventivo y correctivo y la existencia de manuales de procedimientos que permitan realizar las actividades de administración de forma estándar y controlada	[E.21] Errores de mantenimiento / actualización de programas (software)	indisponibilidad - lentitud	4	5	20	A
[HW][host] Servidor de archivos	La ubicación no cuenta con los elementos necesarios para el control de temperatura y humedad necesarios	[I.7] Condiciones inadecuadas de temperatura o humedad	Daño, reducción tiempo vida	2	5	10	M
	No se evidencia la existencia de manuales de procedimientos que permitan realizar las actividades de administración de forma estándar y controlada	[E.2] Errores del administrador	Caída o indisponibilidad	3	5	15	M
	No se evidencia la presencia de planes de mantenimiento preventivo y correctivo y la existencia de manuales de procedimientos que permitan realizar las actividades de administración de forma estándar y controlada	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Caída, mal funcionamiento o indisponibilidad	4	5	20	A
	No se evidencia la existencia de controles de acceso al recurso	[E.25] Pérdida de equipos	Indisponibilidad, robo	2	5	10	M
	No se cuenta con adecuado rack bajo llave	[A.6] Abuso de privilegios de acceso	Falla en la confidencialidad e integridad	3	4	12	M
	Falta de controles de seguridad para el acceso	[A.11] Acceso no autorizado	Robo, perdida o adulteración de información	3	4	12	M

Continuación Tabla 12							
Nombre del activo	**Vulnerabilidad**	**Amenazas**	**Riesgo**	**Probabilidad**	**Impacto**	**valoración**	**Nivel de Riesgo**
[S][int] Servidor de archivos	No se evidencia proceso de control y seguimiento de registros para validar que la información registrada por los usuarios no violenta los acuerdos de privacidad y confidencialidad	[E.1] Errores de los usuarios	Fallas en la confidencialidad y robo	3	2	6	B
	No se evidencia la existencia de manuales de procedimientos que permitan realizar las actividades de administración de forma estándar y controlada	[E.2] Errores del administrador	Caída o indisponibilidad	3	4	12	M
	No se evidencia la existencia de programas de formación y culturización en seguridad informática	[E.19] Fugas de información	Falla en la confidencialidad e integridad	4	5	20	A
	No se cuenta con monitoreo de recursos o manejo de alertas	[E.24] Caída del sistema por agotamiento de recursos	Caída, intermitencia o lentitud	4	5	20	A
	No se cuenta con monitoreo y o seguimiento a actividad de usuarios	[A.5] Suplantación de la identidad del usuario	Falla en la confidencialidad e integridad	4	5	20	A
	No se cuenta con protección de Dos	[A.24] Denegación de servicio	Caída o indisponibilidad	4	5	20	A
[D][files] Servidor de archivos	No se cuenta con registro de actividad y permisos específicos de usuario	[E,14] Escapes de información	Robo o perdida de confidencialidad.	4	5	20	A
	No se evidencia proceso de control y seguimiento de registros para validar que la información registrada por los usuarios no violenta los acuerdos de privacidad y confidencialidad	[E.1] Errores de los usuarios	Fallas en la confidencialidad y robo	4	4	16	A
	No se cuenta con control de cambios o monitoreo de actividades de configuración	[E,15] Alteración accidental de la información	Indisponibilidad o perdida de confidencialidad.	4	5	20	A
	No se tiene trazabilidad de la información alojada ni seguimiento a actividad	[E.19] Fugas de información	Falla en la confidencialidad e integridad	4	5	20	A
	No se cuenta con monitoreo y o seguimiento a actividad de usuarios	[A.6] Abuso de privilegios de acceso	Falla en la confidencialidad e integridad	4	5	20	A
	Falta de controles de seguridad para el acceso	[A.11] Acceso no autorizado	Robo, perdida o adulteración de información	4	5	20	A
	No se cuenta con control de cambios o inventario de información	[A15] Modificación deliberada de la información	perdida de integridad o robo	4	5	20	A

Fuente: El Autor

Se realiza el respectivo análisis de resultados de la matriz de riesgo generada teniendo en cuenta los riesgos de tipo crítico e importante.

Riesgos de nivel crítico.

Se identifica entre los activos de la compañía el firewall, el servicio de internet, página web y la base de datos los cuales cuentan con un nivel de riesgo crítico, por lo que es importante que se Implementen controles basados en la norma ISO 27002:2013 que permitan mitigar los riesgos de cada uno de ellos y ofrezcan la posibilidad de mantener la operación en caso de que una amenaza se materialice.

Riesgo de nivel Importante.

Se identifican activos que presentan un nivel de riesgo alto, muchos de ellos donde se evidencia la falta de documentación de manuales y o guías que puedan disminuir los riesgos asociados a fallas de configuración, también no se observa un plan de capacitación o incentivos de formación al personal técnico de la oficina de TIC lo que puede acarrear que los procesos ejecutados por dicho personal no sean atendidos con tiempos oportunos, adicionalmente no se evidencian procesos documentados para la identificación de vulnerabilidades y tratamiento de estas.

Se observa que no se cuenta con medidas tendientes a evitar que se sustraigan archivos sin previa autorización lo que ocasiona perdida de archivos y que algunos funcionarios por el principio de confidencialidad no deberían conocer. Se evidencia que se debe capacitar al personal sobre buenas prácticas de uso de los recursos informáticos de la oficina. Por otra parte, no se cuenta con una adecuada trazabilidad e identificación de la información alojada sobre los servidores de archivo y sitio web.

Se observa entre el listado de amenazas que tienen un nivel de riesgo alto las asociadas a fallas por parte de los usuarios lo que evidencia una clara falta de

políticas de seguridad y capacitación al personal sobre aspectos de seguridad informática.

6.2 DESARROLLO DE OBJETIVO 2

- INTEGRAR EL DIRECTORIO ACTIVO DE LA COMPAÑÍA B2B TIC SAS AL FIREWALL PERIMETRAL POR MEDIO DE LDAP, PARA FORTALECER Y GENERAR SEGUIMIENTO DE LAS CONEXIONES VPN SSL DE LOS INGENIEROS DE LA COMPAÑÍA.

Para el desarrollo del objetivo se dividen las actividades en fases, las cuales corresponden a:

- **Validación de requerimientos para la integración del directorio activo**

Según el levantamiento de información y activos del objetivo 1 se procede a identificar sobre la Tabla 13 la información más relevante del firewall y directorio activo, entre los cuales se encuentran versiones de servidor, dominios configurados, versión de firmware de firewall y usuarios VPN a fin de continuar con el desarrollo del objetivo 2.

Tabla 13. Información integración directorio activo y firewall

información integración directorio activo a firewall	
información general	
Compañía	B2B TIC SAS
Dirección IP del firewall	192.168.0.1
Información solicitada por	Danilo Alfonso Arias
Fecha	04/05/2020
Comentarios	N/A

Continuación Tabla 13	
Detalle servidor y firewall	
Versión Windows servidor	Windows Server 2016
Bits sistema operativo servidor	64 bits
Dominios	1
Funcionalidades	DIRECTORIO ACTIVO + DNS
Dirección IP	172.16.0.x
Grupos en el directorio activo	4 GRUPOS
Marca de firewall	Fortigate
versión de firmware de firewall	5.6.6
Usuarios vpn actuales	15
VPN SSL	1
Portales acceso tunnel	1
Portales acceso web	0

Fuente: El Autor

Reunida la información básica, se identifican y socializan los requerimientos necesarios para la integración del firewall al directorio activo, los cuales consisten en nuevo usuario con permisos para consultas al servidor LDAP, nuevos grupos y la correspondiente ruta en el árbol como se puede observar sobre la Tabla 14.

Tabla 14. Requerimientos en directorio activo

Información general		
Compañía	B2B TIC SAS	
Requerimiento solicitado por	Danilo Alfonso Arias	
Fecha	11/05/2020	
Comentarios	N/A	
Detalle requerimientos		**Comentario**
Nuevo usuario en servidor ad	Usuario con permiso de lectura sobre el Ad	Para que el Firewall pueda hacer consultas tipo LDAP sobre el servidor de Ad, usuario y la contraseña será solicitada en línea una vez se aplique la configuración sobre el firewall.
Grupos nuevos en servidor	15	Grupos para cada usuario, se debe estandarizar el inicio del nombre del grupo iniciando con VPN_XXXX donde xxxx corresponde al nombre del usuario que está en ese grupo, la finalidad es manejo de autenticación de VPN granular por políticas, se debe indicar la ruta en el árbol para cada grupo

Continuación Tabla 14		
Detalle requerimientos		**Comentario**
Distinguished names	1	confirmar la información del dn del dominio para su configuración en el firewall
Tiempo de indisponibilidad de servidor	0	No es necesario ningún reinicio del servidor, durante el proceso de configuración sobre el firewall no se presentará indisponibilidades.

Fuente: El Autor

Se realiza seguimiento a los requerimientos indicados para la integración del directorio activo y se plasma el estado sobre la Tabla 15, la entrega del usuario para las consultas LDAP será informado durante la actividad de pruebas y se obtiene la relación de grupos con su respectiva ruta del árbol como se observa en la Tabla 16.

A fines de preservar la confidencialidad, a continuación, se realiza el reemplazo sobre todos los cuadros donde se relacione información de grupos o nombres de usuario, desde la segunda letra por x.

Tabla 15. Estado ejecución requerimientos directorio activo

Detalle requerimientos	Estado	Comentario
Nuevo usuario en servidor ad	Creado	información será entregada durante la configuración del Firewall en llamada telefónica
Grupos nuevos en servidor	15	ver Tabla 16
Distinguished names	1	DC= DC=xxxx,DC=loc

Fuente: El Autor

Tabla 16. Relación rutas de grupos en directorio activo

Grupo	Ruta
VPN_dxxxxxx	CN=VPN_dxxxxxx,OU=Usuarios_VPN,OU=ListaGruposGlobal,DC=xxxx,DC=loc
VPN_mxxxxx	CN=VPN_mxxxxx,OU=Usuarios_VPN,OU=ListaGruposGlobal,DC= DC=xxxx,DC=loc
VPN_Jxxxxx	CN=VPN_Jxxxxx,OU=Usuarios_VPN,OU=ListaGruposGlobal,DC= DC=xxxx,DC=loc
VPN_Fxxxxx	CN=VPN_Fxxxxx,OU=Usuarios_VPN,OU=ListaGruposGlobal,DC= DC=xxxx,DC=loc
VPN_Fxxxxx	CN=VPN_Fxxxxx,OU=Usuarios_VPN,OU=ListaGruposGlobal,DC= DC=xxxx,DC=loc
VPN_Jxxxxxx	CN=VPN_Jxxxxxx,OU=Usuarios_VPN,OU=ListaGruposGlobal,DC= DC=xxxx,DC=loc
VPN_Fxxxxxx	CN=VPN_Fxxxxxx,OU=Usuarios_VPN,OU=ListaGruposGlobal,DC= DC=xxxx,DC=loc
VPN_Jxxxxxxx	CN=VPN_Jxxxxxxx,OU=Usuarios_VPN,OU=ListaGruposGlobal,DC= DC=xxxx,DC=loc
VPN_Exxxxxxx	CN=VPN_Exxxxxxx,OU=Usuarios_VPN,OU=ListaGruposGlobal,DC= DC=xxxx,DC=loc
VPN_Jxxxxx	CN=VPN_Jxxxxx,OU=Usuarios_VPN,OU=ListaGruposGlobal,DC= DC=xxxx,DC=loc
VPN_Lxxxxx	CN=VPN_Lxxxxx,OU=Usuarios_VPN,OU=ListaGruposGlobal,DC= DC=xxxx,DC=loc
VPN_Jxxxxxx	CN=VPN_Jxxxxxx,OU=Usuarios_VPN,OU=ListaGruposGlobal,DC= DC=xxxx,DC=loc

Continuación Tabla 16	
Grupo	**Ruta**
VPN_Axxxx	CN=VPN_Axxxx,OU=Usuarios_VPN,OU=ListaGruposGlobal,DC= DC=xxxx,DC=loc
VPN_Mxxxxxx	CN=VPN_Mxxxxxx,OU=Usuarios_VPN,OU=ListaGruposGlobal,DC= DC=xxxx,DC=loc
VPN_Ixxxxxx	CN=VPN_Ixxxxxx,OU=Usuarios_VPN,OU=ListaGruposGlobal,DC= DC=xxxx,DC=loc

Fuente: El Autor

- **Planeación y ejecución de actividades de preconfiguración.**

Con la información correspondiente a los grupos de usuarios se realiza un plan de actividades en el cual se registran los tiempos aproximados y configuraciones a aplicar como se detalla en la Tabla 17. Junto a él se listan sobre la Tabla 18 las políticas a configurar por cada grupo.

Tabla 17. Actividades configuración firewall

Numero actividad	Descripción Actividades	Duración
1.Toma de backup	Tomar backup de configuración del Firewall	10 min
2.Validación estado actual firewall	Tomar registro de estado actual del firewall en cuanto a los recursos de CPU/memoria	20 min
3.Integración LDAP en firewall	Sobre el firewall ingresar al menu User & Device > LDAP server > Create New, adicionar los datos del servidor de Ad y contactar al personal de TIC para solicitar información de usuario y contraseña del usuario requerido para la integración.	20 min
5.Adición de grupos según rutas	Creación de grupos según la tabla 16	30 min
6.Adición de grupos a portal	Adición grupos a portal VPN	20 min
7.Adición de políticas	Creación de políticas para los grupos, se dejan deshabilitadas para posterior a esto generar pruebas (tabla18)	30 min
8.Toma de backup	Tomar backup de configuración del Firewall posterior a los cambios ejecutados	10 min
9.Validación estado actual firewall	Tomar registro de estado actual del firewall en cuanto a los recursos de CPU/memoria.	20 min
10.Fin actividad	Confirmación de normalidad para los usuarios que actualmente se conectan por la VPN y tienen navegación por el firewall.	15 min
Duración total en minutos		185 min

Fuente: El Autor

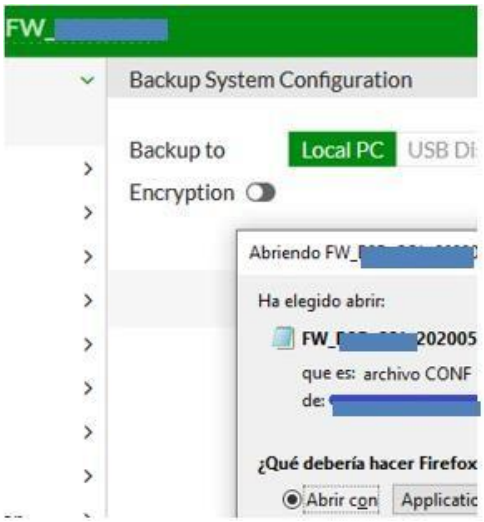
Tabla 18. Relación de políticas

Políticas Firewall				
Nombre	**Grupo**	**Servicio**	**Red Origen**	**Red destino**
Ssl_User1	VPN_dxxxxxx	Rdp	Vpn_Ssl	LAN
Ssl_User2	VPN_mxxxxx	Rdp	Vpn_Ssl	LAN
Ssl_User3	VPN_Jxxxxx	Rdp	Vpn_Ssl	LAN
Ssl_User4	VPN_Fxxxxx	Rdp	Vpn_Ssl	LAN
Ssl_User5	VPN_Fxxxxx	Rdp	Vpn_Ssl	LAN
Ssl_User6	VPN_Jxxxxxx	Rdp	Vpn_Ssl	LAN
Ssl_User7	VPN_Fxxxxxx	Rdp	Vpn_Ssl	LAN
Ssl_User8	VPN_Jxxxxxxx	Rdp	Vpn_Ssl	LAN
Ssl_User9	VPN_Exxxxxxx	Rdp	Vpn_Ssl	LAN
Ssl_User10	VPN_Jxxxxx	Rdp	Vpn_Ssl	LAN
Ssl_User11	VPN_Lxxxxx	Rdp	Vpn_Ssl	LAN
Ssl_User12	VPN_Jxxxxxx	Rdp	Vpn_Ssl	LAN
Ssl_User13	VPN_Axxxx	Rdp	Vpn_Ssl	LAN
Ssl_User14	VPN_Mxxxxxx	Rdp	Vpn_Ssl	LAN
Ssl_User15	VPN_Ixxxxxx	Rdp	Vpn_Ssl	LAN

Fuente: El Autor

Se inicia la actividad de preconfiguración sobre el firewall según lo planeado, tomando un backup de configuración como se observa sobre la Figura 3 y posterior dando ejecución a las actividades propuestas.

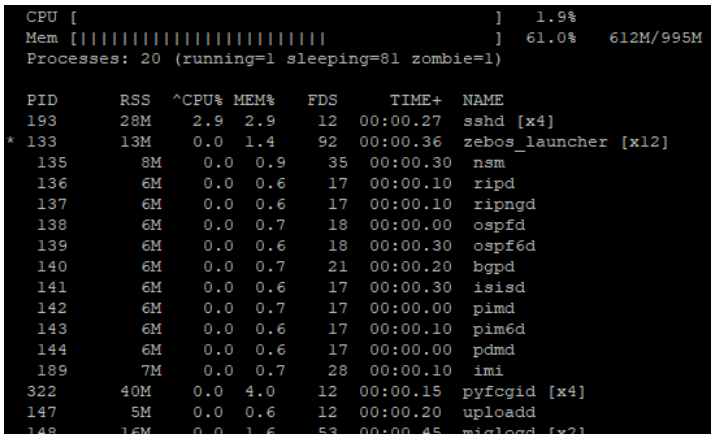
Figura 3. Toma backup firewall



Fuente: El Autor

Con base a lo planteado se realiza la ejecución de comandos a fin de monitorear los recursos de memoria y CPU sobre el firewall, donde se evidencia luego de unos minutos un promedio de 2% de CPU y 61% de memoria como se registra sobre la Figura 4 en las líneas de Mem y CPU.

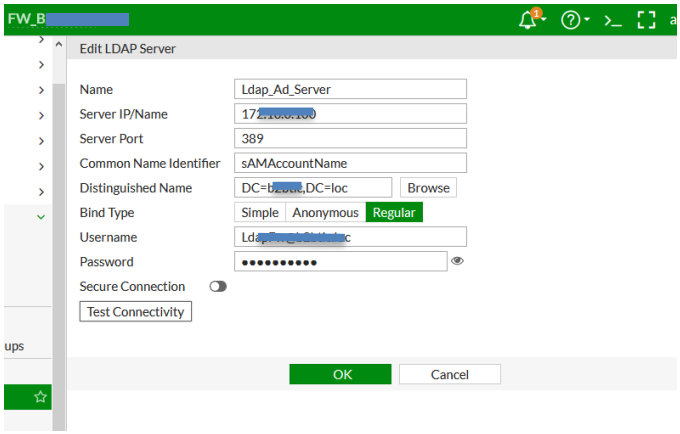
Figura 4. Estado recursos firewall



Fuente: El Autor

A continuación, en la Figura 5 se realiza la configuración del servidor LDAP sobre el firewall, ingresando la dirección IP, distinguished name y usuario con permisos para las consultas LDAP con su correspondiente contraseña.

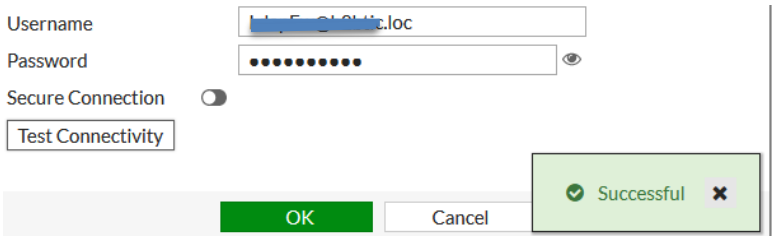
Figura 5. Configuración LDAP server en firewall



Fuente: El Autor

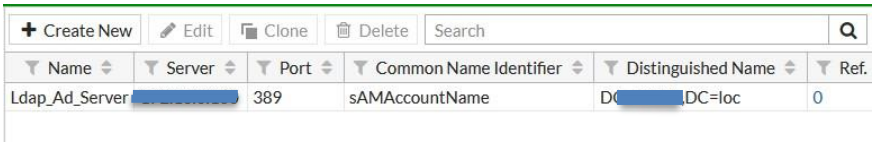
Una vez configurado el servidor LDAP se realizan pruebas de conexión las cuales son exitosas como se observa sobre la Figura 6, posteriormente al darle ok sobre el menú se observa que fue correctamente adicionado a la configuración como registra la Figura 7. Por último, se intenta crear un grupo seleccionando el servidor LDAP configurado evidenciando que se hace la consulta y visualización de los grupos de una forma correcta como se puede ver en la Figura 8.

Figura 6. Prueba servicio LDAP



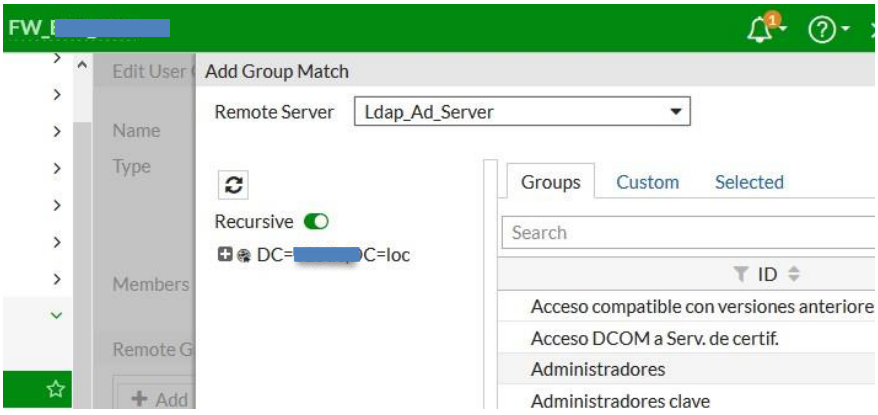
Fuente: El Autor

Figura 7. Servidor LDAP en firewall



Fuente: El Autor

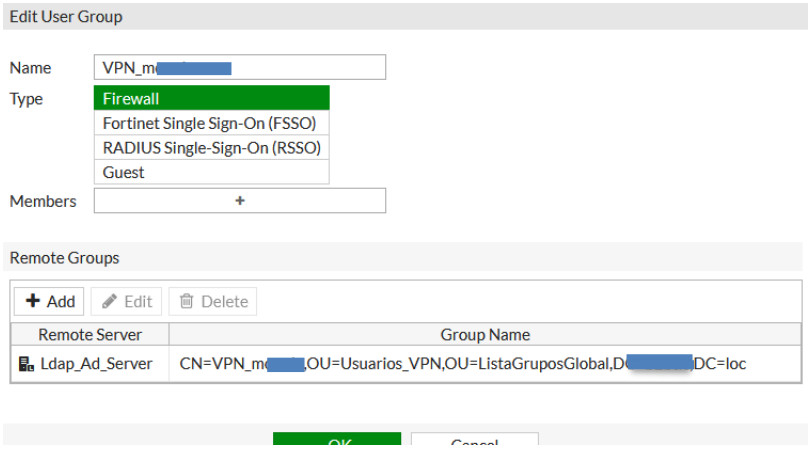
Figura 8. Validación árbol de directorio activo



Fuente: El Autor

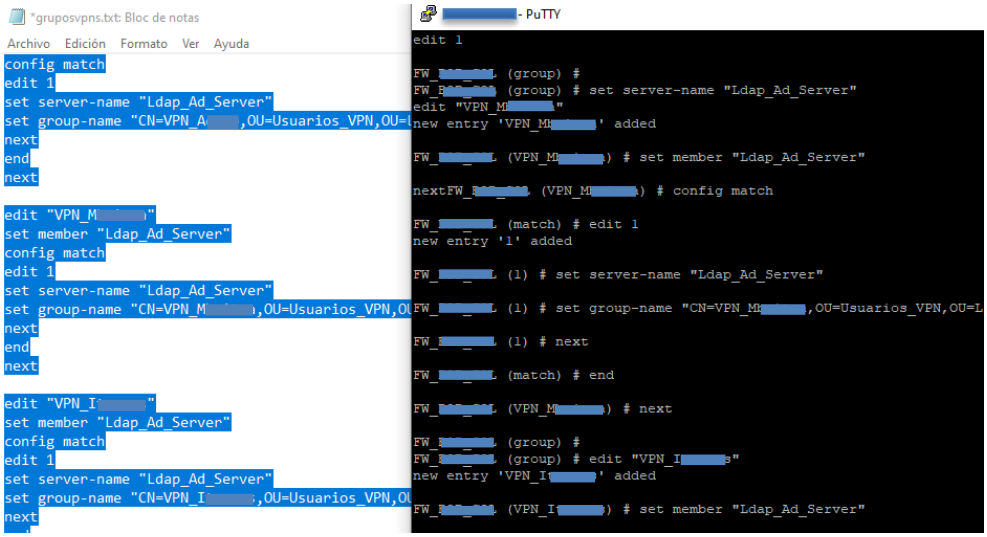
Una vez la integración del LDAP con el firewall es correcta se procede a realizar la configuración de cada uno de los grupos, uno vía GUI ingresando nombre, seleccionado el servidor LDAP y ruta como se observa en la Figura 9, los demás vía CLI mediante un script de configuración como se evidencia en la Figura 10, finalmente sobre la Figura 11 se puede ver el listado de grupos configurados sobre el firewall.

Figura 9. Creación usuario vía GUI



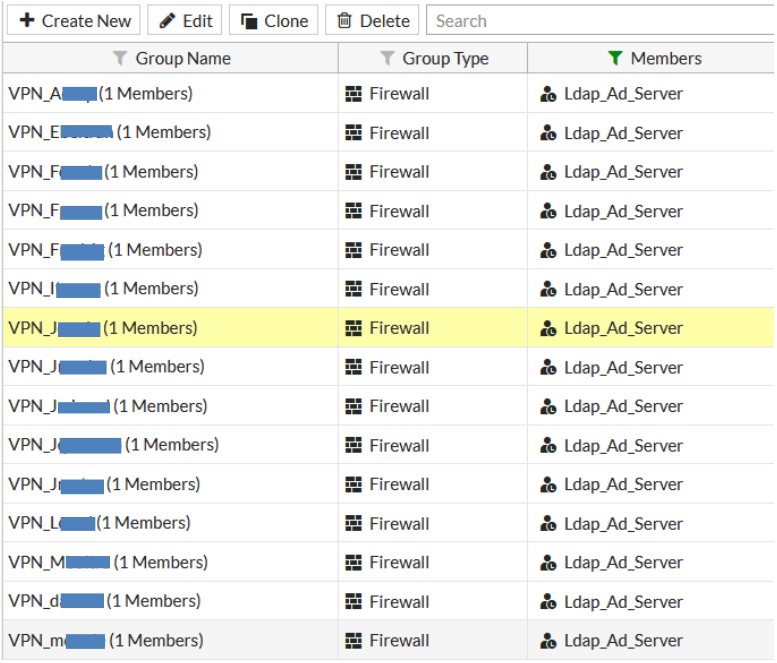
Fuente: El Autor

Figura 10. Creación usuarios vía CLI



Fuente: El Autor

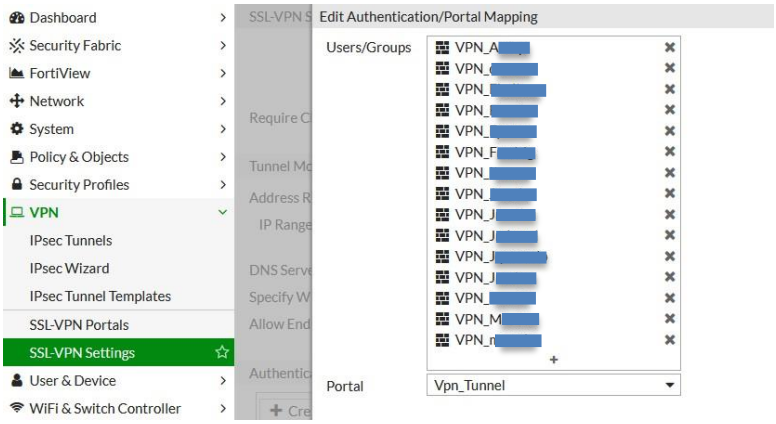
Figura 11. Relación usuarios configurados



Fuente: El Autor

Una vez los grupos se encuentran creados se adicionan a la configuración de VPN SSL y se selecciona su correspondiente portal, como se registra en la Figura 12.

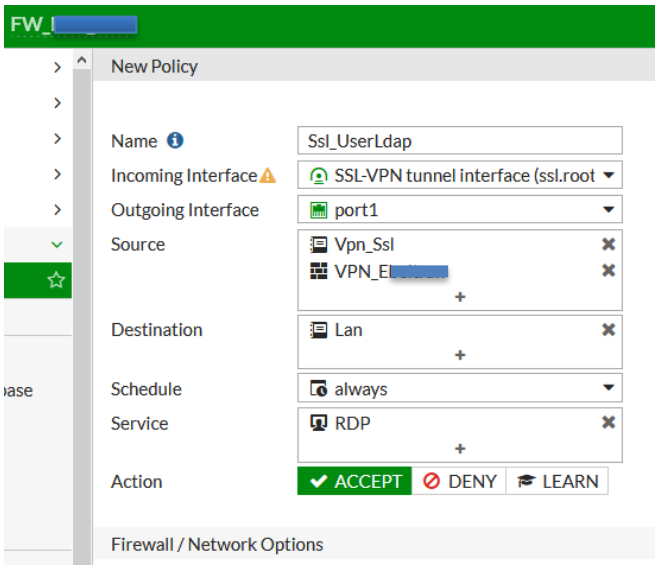
Figura 12. Adición usuarios a VPN SSL



Fuente: El Autor

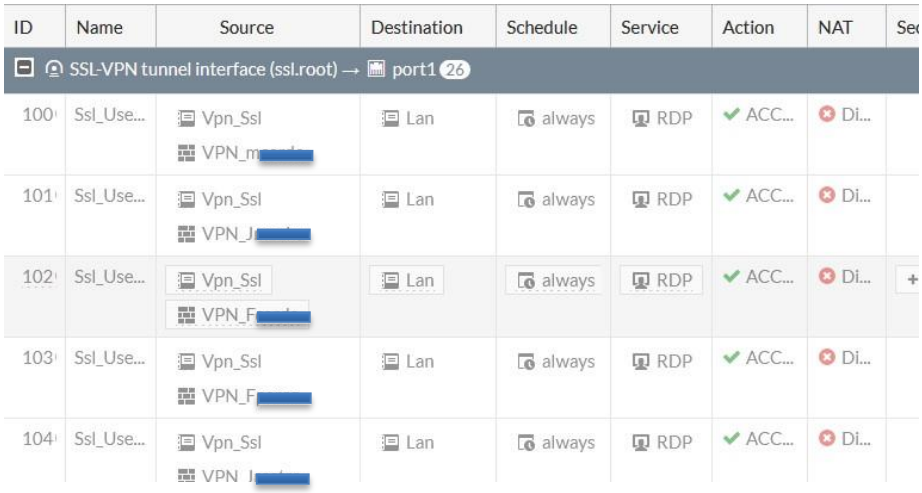
Se inicia la configuración de las políticas para cada grupo al definir las interfaces de entrada y salida, grupo de usuario, dirección IP origen-destino y servicio, como se observa en la Figura 13. Posterior a ello se procede a deshabilitar las políticas en la configuración del firewall y se visualiza su estado como se registra en la Figura 14.

Figura 13. Creación política vía GUI



Fuente: El Autor

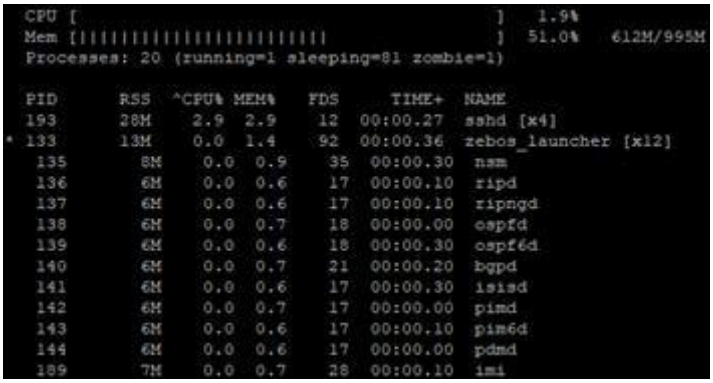
Figura 14. Vista políticas configuradas



Fuente: El Autor

Luego de aplicar la configuración de políticas se procede a revisar el estado del firewall en CPU y memoria, los cuales registran parámetros normales 1.9% CPU y 51% Memoria como se evidencia en la Figura 15 en las líneas de Mem y CPU.

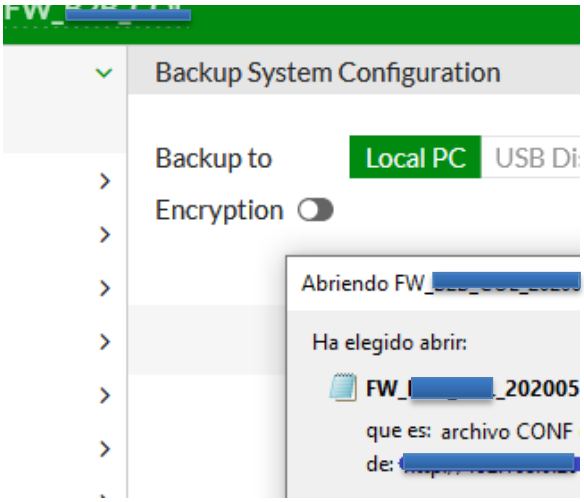
Figura 15. Estado recursos firewall



Fuente: El Autor

Al finalizar se realiza una nueva toma de backup de configuración del firewall con el fin de tener respaldo de la configuración aplicada, como se puede observar sobre la Figura 16, por último, se confirma normalidad sobre los servicios que cursan sobre el firewall con los usuarios.

Figura 16. Backup configuración firewall



Fuente: El Autor

- **Ejecución de pruebas de integración de directorio activo y autenticación de usuarios vía VPN**.

Posterior a las preconfiguraciones se realiza solicitud para ejecutar actividades de pruebas, las cuales consisten en activar las políticas creadas y confirmar que los usuarios VPN puedan autenticarse de una forma satisfactoria, dichas actividades son descritas sobre la Tabla 19.

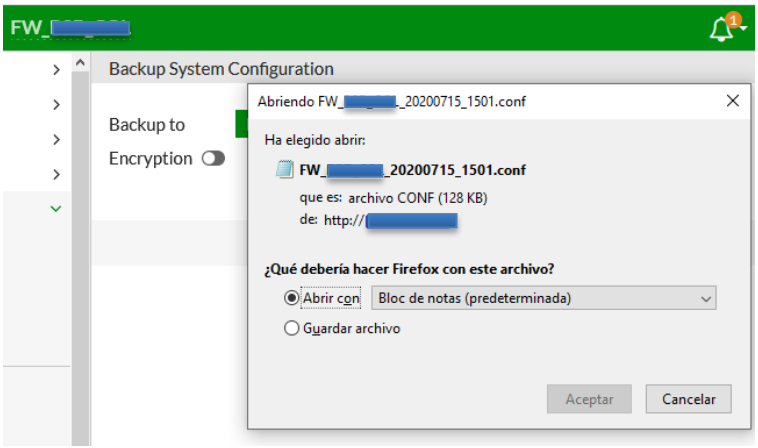
Tabla 19. Actividades pruebas usuarios VPN

Numero Actividades	Descripción Actividades	Duración
1.Toma de backup	Tomar backup de configuración del Firewall	5 min
2.Validación estado actual firewall	Tomar registro de estado actual del firewall en cuanto a los recursos de CPU/memoria	5 min
3, Conferencia	Establecer comunicación telefónica para inicio de pruebas ingenieros mxxxxx y jxxxxxx, y personal administrador del AD	5 min
4.Habilitación de políticas	habilitar las reglas para los usuarios mxxxxx y jxxxxxx	5 min
5.Conexión usuarios	Pruebas de conexión de los ingenieros con su usuario y contraseña de dominio, pruebas de acceso a recursos.	20 min
6.Validaciones	Validación sobre Firewall y directorio activo	10 min
7.Toma de backup	Tomar backup de configuración del Firewall posterior a los cambios ejecutados	5 min
8.Fin actividad	Confirmación de normalidad para los usuarios que actualmente se conectan por la VPN y tienen navegación por el firewall.	5 min
Duración total en minutos		60 min

Fuente: El Autor

Una vez se cuenta con la autorización, se procede a ejecutar las actividades de pruebas planteadas anteriormente, dando inicio con la toma de backup de configuración del firewall como se puede observar en la Figura 17.

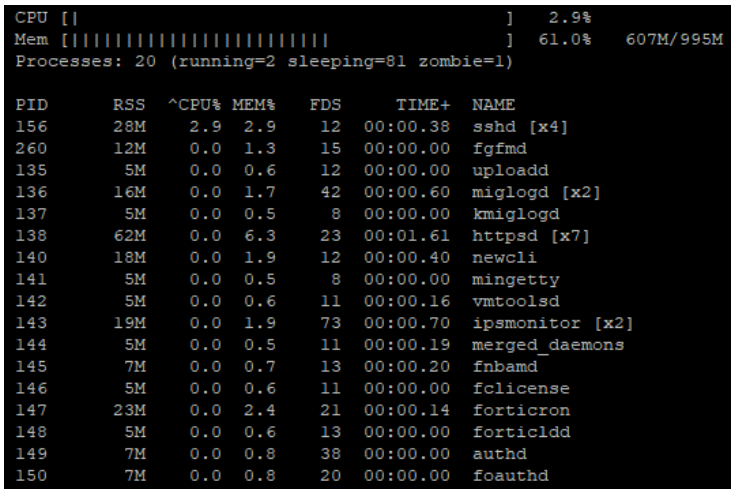
Figura 17. Backup configuración



Fuente: El Autor

Dando continuidad a las actividades se procede a realizar una toma del estado actual de los recursos sobre el firewall, como se evidencia en la Figura 18 registrando promedio de memoria de 61% y CPU 2.9%.

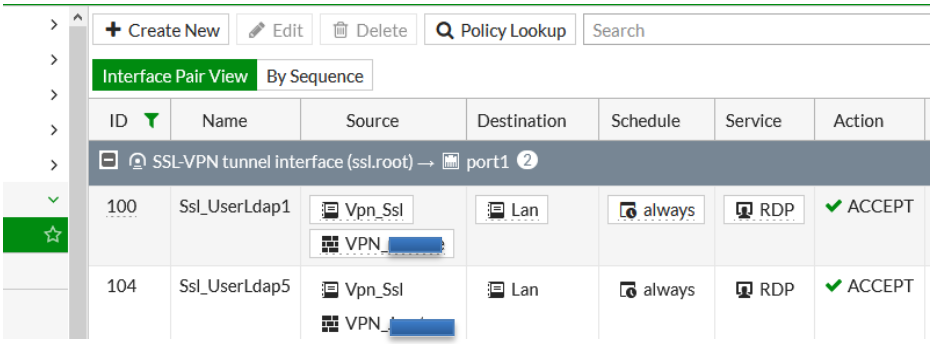
Figura 18. Estado recursos firewall



Fuente: El Autor

Posterior a la toma de backup se indica a los ingenieros las pruebas que se requieren y se procede a habilitar las políticas correspondientes a los usuarios mxxxxx y jxxxxxx sobre la configuración firewall por el entorno gráfico GUI como se puede evidenciar sobre la Figura 19.

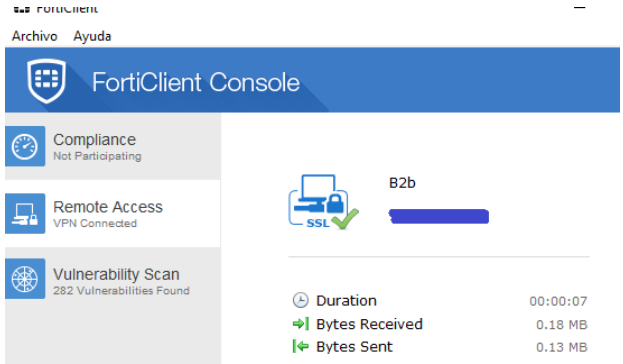
Figura 19. Habilitación de políticas



Fuente: El Autor

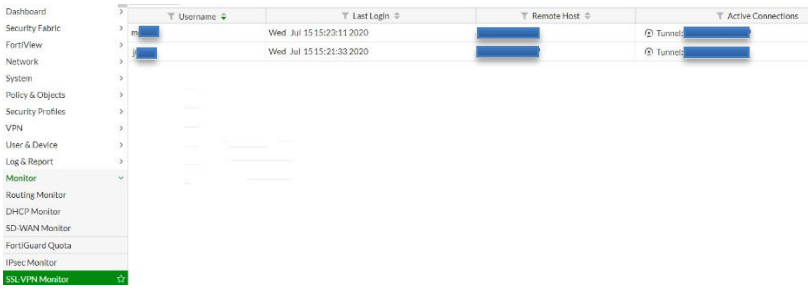
Por parte de los ingenieros que tienen asignados los usuarios mxxxxx y jxxxxxx se realiza la autenticación con el usuario y contraseña de dominio de forma exitosa por medio del FortiClient como se observa en la Figura 20, de esta manera sobre el monitoreo de conexiones VPN del firewall se evidencia la conexión activa de los usuarios como se registra en la Figura 21. Por último, se valida con los usuarios el correcto acceso a los servidores en la lan y se observa conteo de tráfico en las políticas como se evidencia sobre la Figura 22.

Figura 20. Conexión usuario VPN



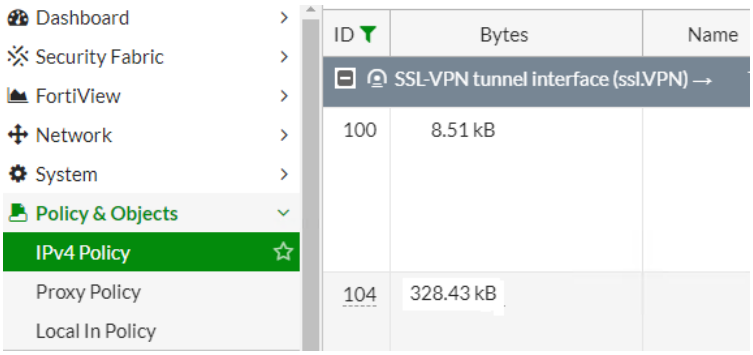
Fuente: El Autor

Figura 21. Registro conexión usuario VPN



Fuente: El Autor

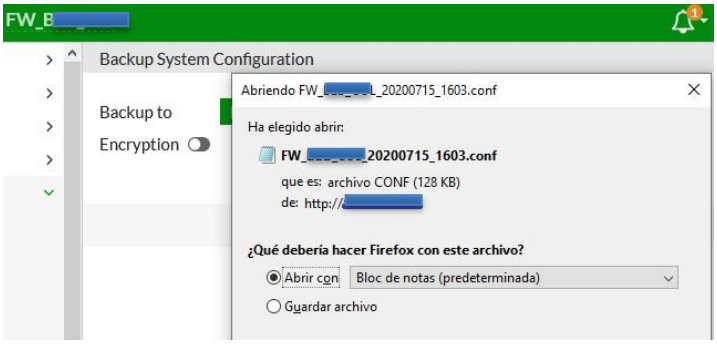
Figura 22. Registro de tráfico sobre políticas



Fuente: El Autor

Después de confirmar y tomar evidencias del resultado exitoso de las pruebas, se procede a tomar un backup de la configuración del firewall como se registra en la Figura 23.

Figura 23. Toma backup fin actividad



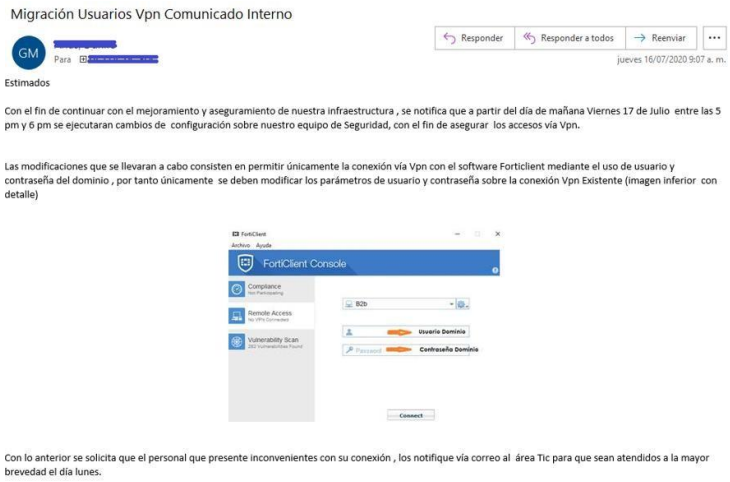
Fuente: El Autor

- **Puesta en marcha de autenticación de usuarios vía VPN mediante LDAP.**

Al tener el resultado de las pruebas, las cuales fueron exitosas, se procede a la activación de las políticas preconfiguradas y junto a ello realizar la respectiva baja de los usuarios locales del firewall utilizados para la conexión VPN.

Se genera una notificación interna vía correo para los usuarios que utilizan la conexión vía VPN, donde se informan las modificaciones a ejecutar y los datos que se deben ingresar para la conexión, como se observa en la Figura 24.

Figura 24. Comunicado usuarios VPN



Fuente: El Autor

Posteriormente se genera un plan de actividades con 7 ítems, como se observa sobre la Tabla 20, donde se describe cada uno de los pasos a ejecutar durante la puesta en producción, dando inicio con validaciones sobre el estado de firewall para continuar con activación de políticas, depuración de usuarios y las pruebas de conexión de usuarios VPN. Para finalmente contar con la autenticación vía LDAP de todos los usuarios VPN.

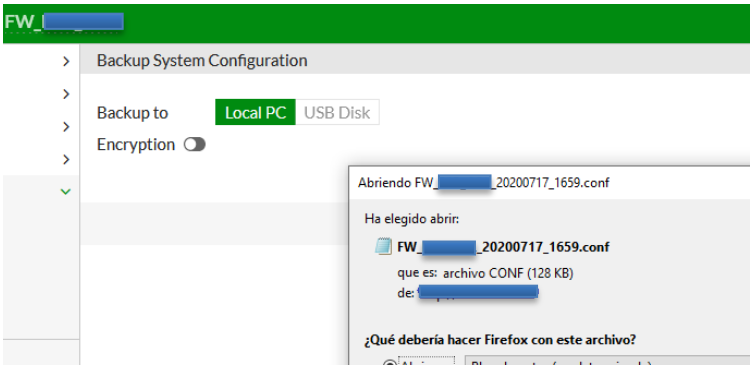
Tabla 20. Actividades puestas en marcha autenticación LDAP

Numero Actividades	Descripción actividades	Duración
1.Toma de backup	Tomar backup de configuración del Firewall	5 min
2.Validación estado actual firewall	Tomar registro de estado actual del firewall en cuanto a los recursos de CPU/memoria	5 min
3.Activación de políticas	Activación de políticas correspondientes a usuarios dxxxxxx, Jxxxxx, Fxxxxx, Fxxxxx, Fxxxxxx, Jxxxxxxx, Exxxxxxx, Jxxxxx, Lxxxxx, Jxxxxxx, Axxxx, Mxxxxxx, Ixxxxxx	15 min
4.Eliminación usuarios locales	Eliminación usuarios locales del portal y remoción de configuración	15min
5.Prueba conexión	Se generan pruebas de conexión con un usuario	5 min
6.Toma de backup	Tomar backup de configuración del Firewall posterior a los cambios ejecutados	5 min
6.Validación estado actual firewall	Tomar registro de estado actual del firewall en cuanto a los recursos de CPU/memoria.	5 min
7.Fin actividad	Confirmación de normalidad para los usuarios que actualmente se conectan por la VPN	5 min
Duración total en minutos		60 min

Fuente: El Autor

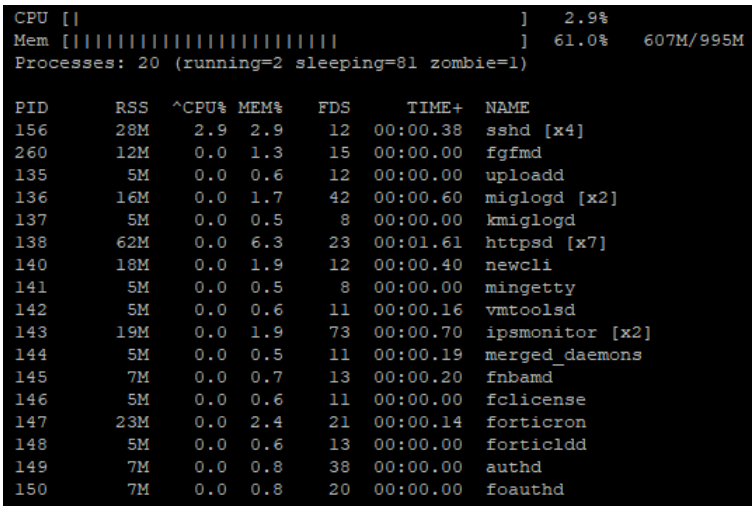
Una vez aprobadas las actividades se da inicio con la toma de backup de la configuración del firewall como se observa sobre la Figura 25, seguido a ello se revisa el estado de recursos del firewall, el cual cuenta con valores normales de CPU y memoria como se evidencia en la Figura 26.

Figura 25. Toma backup inicio actividad



Fuente: El Autor

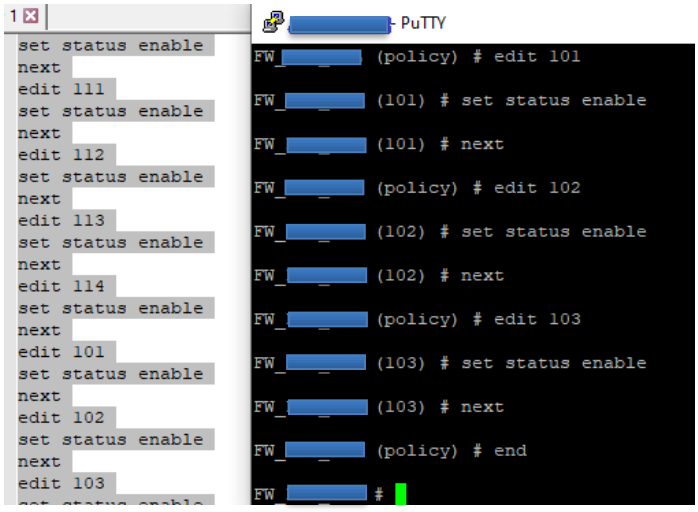
Figura 26. Estado recursos firewall



Fuente: El Autor

Se ejecuta la actividad correspondiente a la activación de políticas, por medio de una conexión SSH al firewall mediante un script de configuración, el cual consiste en la activación de las políticas para los usuarios que se encontraban pendientes como se registra en la Figura 27.

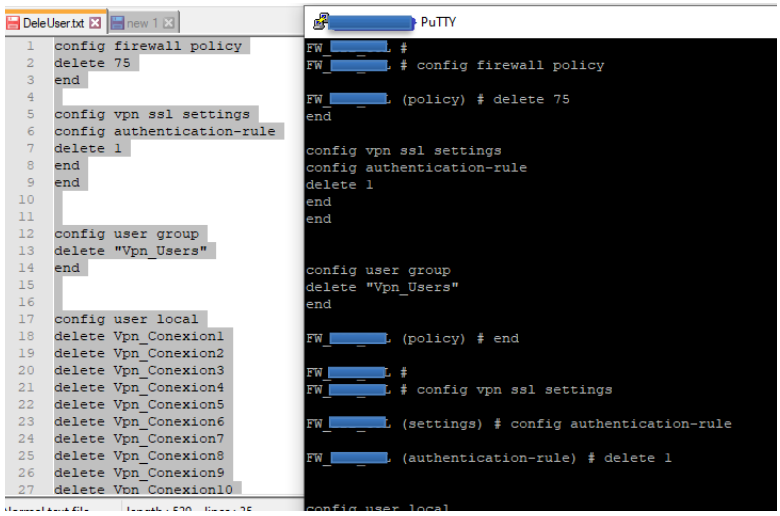
Figura 27. Activación de políticas



Fuente: El Autor

Para la actividad número 4. Se elimina la política asociada a los usuarios locales y posteriormente se remueve el grupo del portal actual, se elimina el grupo para finalmente realizar la depuración de los usuarios. Esta actividad se realiza por medio de un script como se observa en la Figura 28.

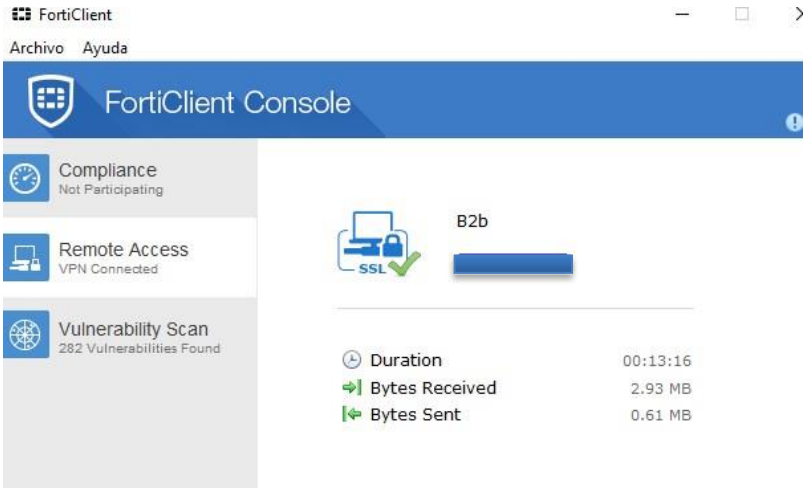
Figura 28. Eliminación usuarios locales



Fuente: El Autor

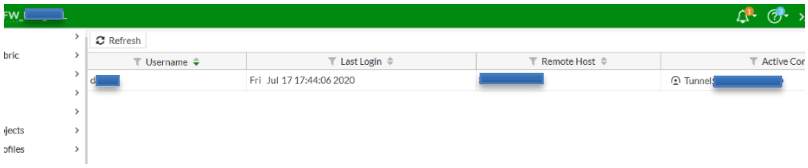
Se realizan las pruebas de conexión correspondientes con un usuario VPN por medio de FortiClient donde se evidencia que la conexión es exitosa, como se observa en la Figura 29. Posterior a ello en el monitoreo de usuarios del firewall se registra la autenticación y evidencia acceso a los recursos de la red LAN de la compañía como lo muestra la Figura 30.

Figura 29. Conexión usuario VPN



Fuente: El Autor

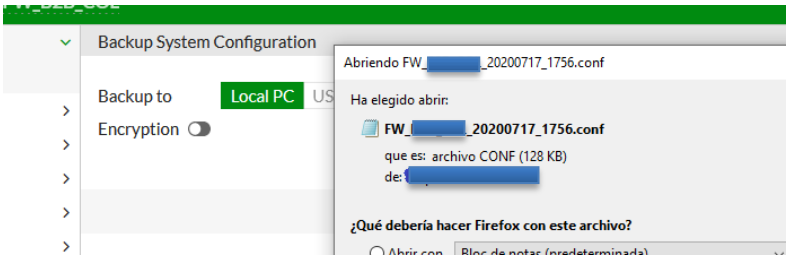
Figura 30. Registro conexión usuario VPN



Fuente: El Autor

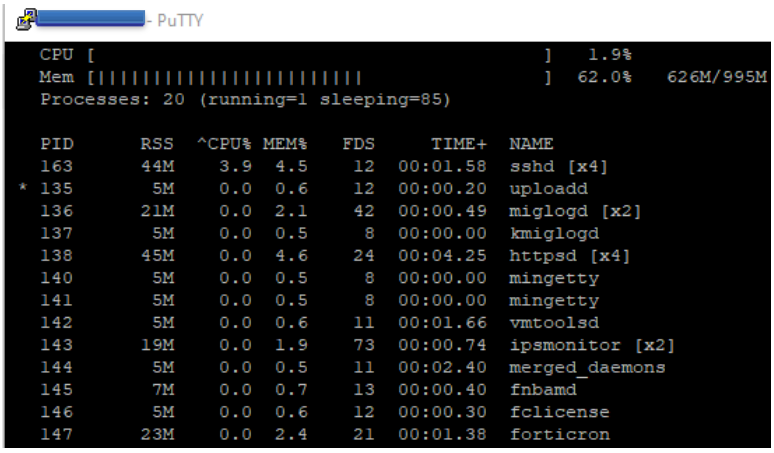
Al finalizar la actividad se toma backup de configuración del firewall como se registra sobre la Figura 31 y se vuelve a monitorear el estado de los recursos como se observa sobre la Figura 32, donde se evidencian parámetros normales de CPU y memoria.

Figura 31. Toma backup fin actividad



Fuente: El Autor

Figura 32. Estado recursos firewall



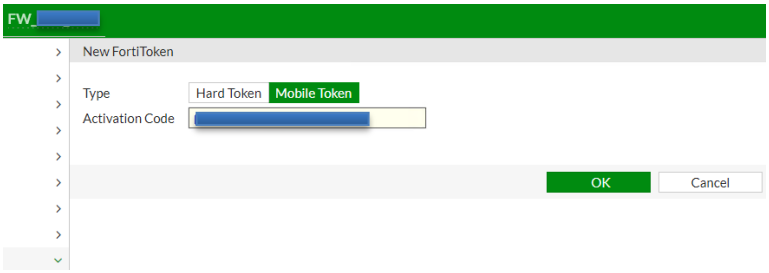
Fuente: El Autor

- **Asignación de Token para segunda capa de seguridad**

Una vez los usuarios ya cuentan con autenticación por medio del directorio activo, se procede a generar la asignación de tokens para tener una segunda capa de seguridad, para ello se cuenta con un demo de 5 tokens móviles a los cuales se les conoce como FortiToken Mobile según el nombre asignado por el fabricante.

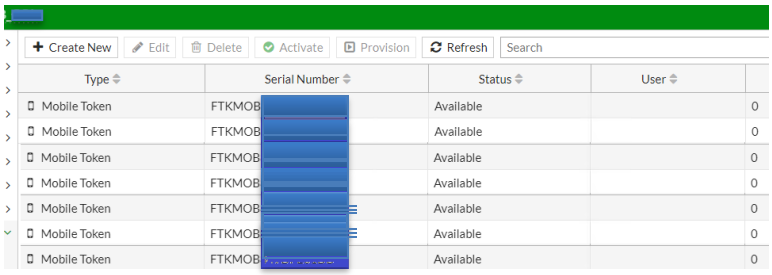
La licencia demo de los 5 FortiToken Mobile fue tramitado por la gerencia y junto con ellos se cuenta con dos tokens gratuitos precargados al firewall por parte del fabricante, con ello se inicia el proceso de integración.
Mediante el serial entregado para el demo, se realiza el respectivo cargue sobre el firewall, se ingresa al menú de FortiToken se selecciona la opción de Mobile Token y se ingresa el serial en la casilla de activation code como se registra en la Figura 33, finalmente al aplicar el código se observa que los tokens son visualizados sobre la configuración del firewall como se evidencia sobre la Figura 34.

Figura 33. Cargue serial para FortiTokens



Fuente: El Autor

Figura 34. FortiTokens cargados



Fuente: El Autor

Se confirma con gerencia 5 usuarios que deben contar con el doble factor de autenticación, los cuales son registrados sobre la Tabla 21. Adicionalmente se recibe notificación de fecha para las configuraciones y pruebas, previo a ello se debe generar una lista de actividades las cuales son relacionadas sobre la Tabla 22 y un manual básico para que los usuarios realicen el proceso de activación de los FortiToken Mobile (Anexo 5) a fin de lograr la autenticación vía VPN.

Tabla 21. Usuarios para asignación de tokens

Usuario
Fxxxxx
Jxxxxxx
Fxxxxxx
Jxxxxxxx
Exxxxxxx

Fuente: El Autor

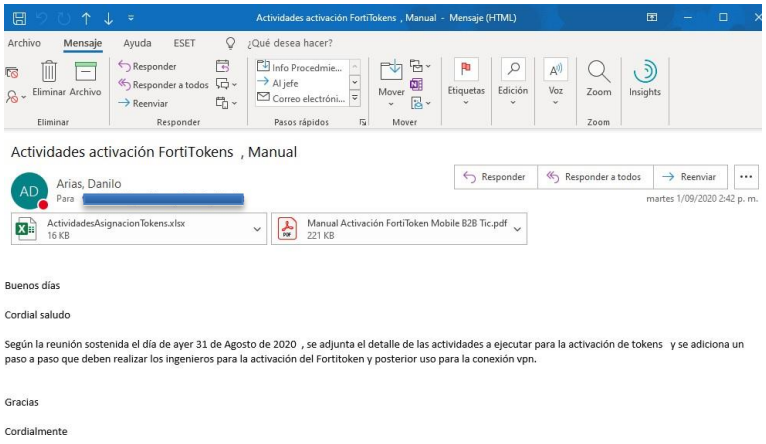
Tabla 22. Actividades asignación tokens y pruebas

Numero Actividades	Descripción actividades	Duración
1.Toma de backup	Tomar backup de configuración del Firewall	5 min
2.Validación estado actual firewall	Tomar registro de estado actual del firewall en cuanto a los recursos de CPU/memoria	5 min
3.Asignación de token	Asignación de token a 5 usuarios	20 min
4.Activación de token usuario	Activación de token	25 min
5.Prueba conexión	Autenticación vía VPN con credenciales de dominio y token	20 min
6.Toma de backup	Tomar backup de configuración del Firewall posterior a los cambios ejecutados	5 min
7.Validación estado actual firewall	Tomar registro de estado actual del firewall en cuanto a los recursos de CPU/memoria.	5 min
8.Fin actividad	Confirmación de normalidad para los usuarios que actualmente se conectan por la VPN	5 min
Duración total en minutos		90 min

Fuente: El Autor

Por medio de mensaje de correo se notifican los detalles de la actividad de puesta en marcha de los tokens, junto con el manual generado como se evidencia en la Figura 35.

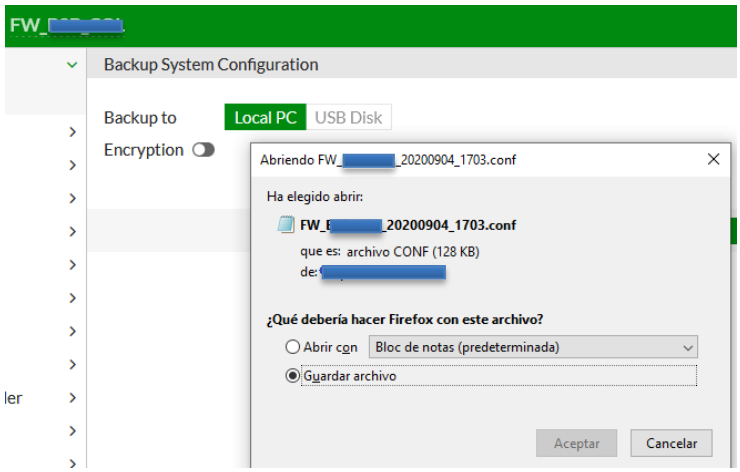
Figura 35. Detalle actividades y manual FortiToken



Fuente: El Autor

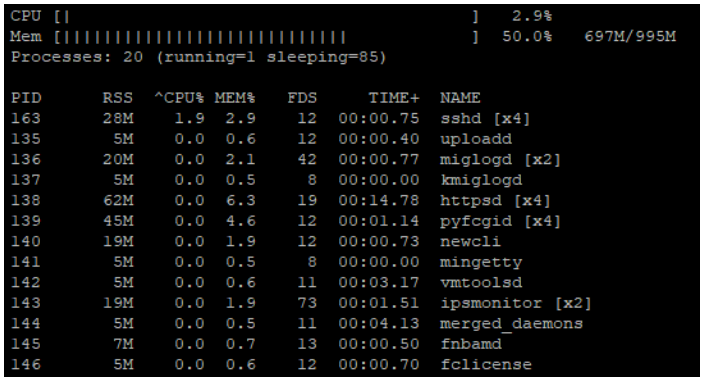
Se procede a iniciar con las actividades definidas, con una toma de backup de configuración del firewall como se observa en la Figura 36, para posteriormente validar el estado de recursos de CPU y memoria los cuales se encuentran dentro de parámetros normales como se evidencia sobre la Figura 37.

Figura 36. Toma backup inicio actividad



Fuente: El Autor

Figura 37. Estado recursos firewall

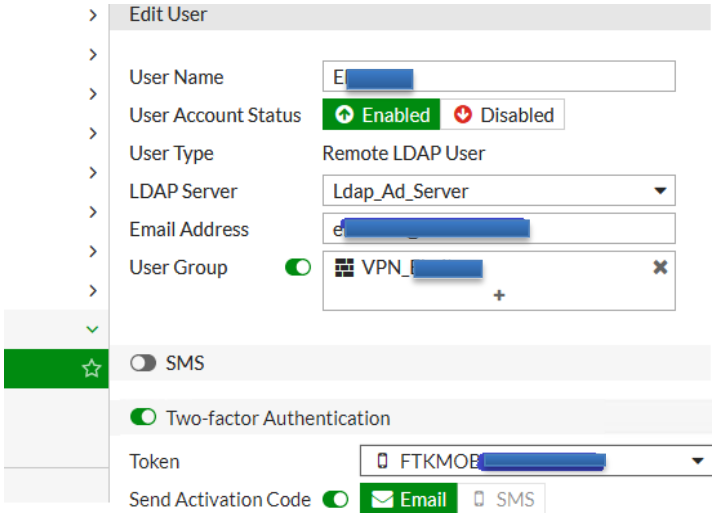


Fuente: El Autor

Se continúa con la actividad número 3. Se asigna el token correspondiente a cada uno de los 5 usuarios sobre el firewall y se selecciona la opción para que se haga envió de los datos de activación vía mensaje de correo como se evidencia en la

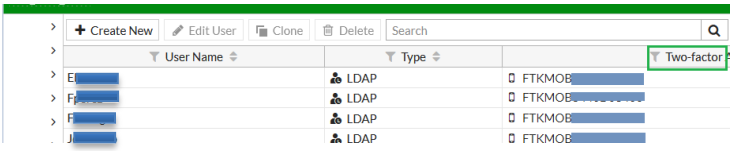
Figura 38, al finalizar es posible observar el listado de usuarios del firewall el token asignado para cada uno como se observa sobre la Figura 39 y en el menú de FortiToken su estado en Pending como se registra en la Figura 40, que corresponde a que está pendiente por activación.

Figura 38. Asignación tokens



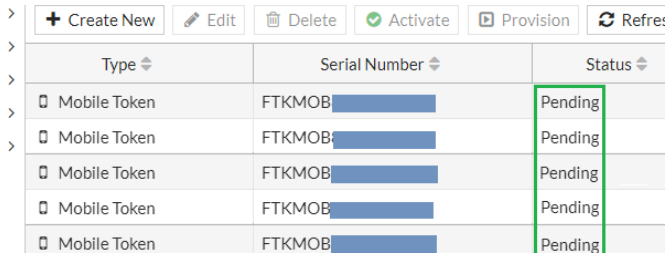
Fuente: El Autor

Figura 39. Relación tokens por usuario



Fuente: El Autor

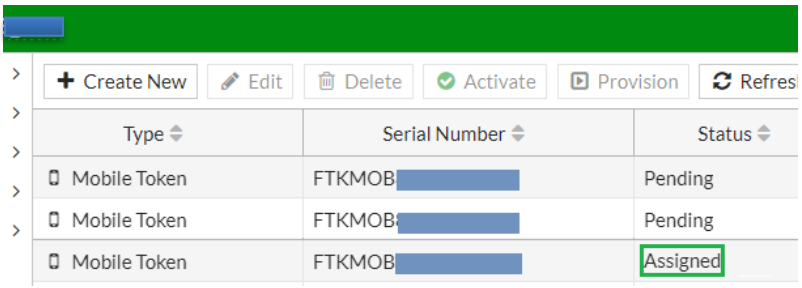
Figura 40. Estado de FortiToken asignados



Fuente: El Autor

Para la actividad 4, activación de tokens de usuario se solicita a los ingenieros seguir el manual enviado vía correo electrónico, con el asunto “Manual Activación FortiToken Mobile B2B TIC”, una vez el usuario culmina el proceso de activación se observa que el estado del token pasa a Assigned como se registra en la Figura 41.

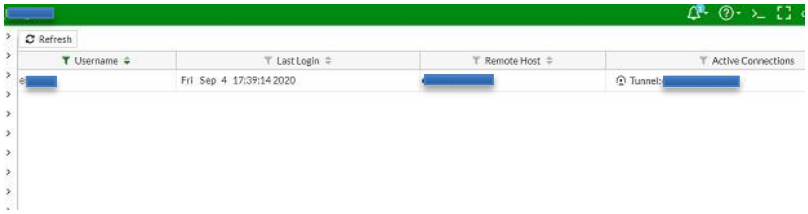
Figura 41. Eliminación usuarios locales



Fuente: El Autor

El token ya se encuentra asignado y activado por lo que se procede con el paso 5, donde el usuario realiza la conexión con el FortiClient a la VPN corporativa ingresando el usuario y contraseña de dominio para posteriormente observar que la VPN solicita el segundo factor de autenticación el cual corresponde al token visualizado en el FortiToken Mobile, una vez ingresado el segundo factor de autenticación se observa que la conexión es exitosa, se valida sobre el monitoreo de conexiones VPN en el firewall la autenticación correcta, como se observa sobre la Figura 42.

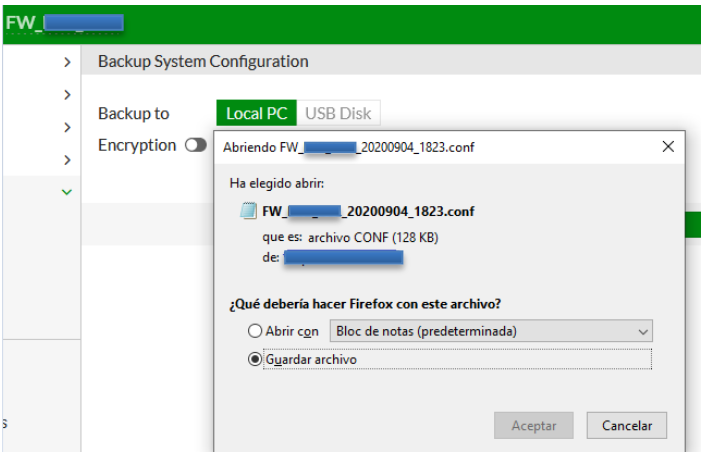
Figura 42. Conexión usuario VPN



Fuente: El Autor

Se ejecutan los pasos 6 y 7 para dar por finalizada la actividad de una manera satisfactoria, el mismo proceso que ejecuto el usuario en base al manual debe ser ejecutado por los 4 usuarios faltantes, se realiza toma de backup de configuración del firewall como se evidencia sobre la Figura 43 y se realiza una revisión del estado de los recursos del equipo en cuanto a CPU y memoria, los cuales se visualizan entre los parámetros normales de operación como se observa sobre la Figura 44.

Figura 43. Toma backup fin actividad



Fuente: El Autor

Figura 44. Estado recursos firewall fin actividad

```
CPU [                                        ]   1.9%
Mem [||||||||||||||||||||||||||              ]  60.0%   702M/995M
Processes: 20 (running=1 sleeping=85)

PID      RSS   ^CPU% MEM%   FDS     TIME+  NAME
163      29M    2.9  2.9    12  00:01.40  sshd [x4]
135       5M    0.0  0.6    12  00:00.60  uploadd
136      20M    0.0  2.1    42  00:01.10  miglogd [x2]
137       5M    0.0  0.5     8  00:00.00  kmiglogd
138      75M    0.0  7.6    22  00:19.94  httpsd [x4]
139      45M    0.0  4.6    12  00:01.28  pyfcgid [x4]
140      19M    0.0  1.9    12  00:01.00  newcli
141       5M    0.0  0.5     8  00:00.00  mingetty
142       5M    0.0  0.6    11  00:04.27  vmtoolsd
143      19M    0.0  1.9    73  00:02.30  ipsmonitor [x2]
144       5M    0.0  0.5    11  00:05.68  merged_daemons
145       7M    0.0  0.7    13  00:00.60  fnbamd
146       5M    0.0  0.6    12  00:00.90  fclicense
147      23M    0.0  2.4    21  00:03.38  forticron
151       5M    0.0  0.6    13  00:00.90  forticldd
152       7M    0.0  0.8    38  00:00.20  authd
153       7M    0.0  0.8    20  00:00.10  foauthd
154       4M    0.0  0.5     9  00:00.00  httpclid
155      27M    0.0  2.8    15  00:01.72  reportd
156      19M    0.0  2.0    29  00:00.21  sslvpnd
```

Fuente: El Autor

6.3 DESARROLLO DE OBJETIVO 3

- DEFINIR LAS POLÍTICAS DE SEGURIDAD PARA EL CONTROL DE ACCESO DE LOS USUARIOS VÍA VPN, CON EL FIN DE QUE SEAN DOCUMENTADAS Y SOCIALIZADAS EN EL RESPECTIVO PROCESO DE INDUCCIÓN DEL PERSONAL NUEVO O REINDUCCIÓN PARA EL PERSONAL EXISTENTE.

Las políticas fueron diseñadas para el control de acceso teniendo como base el dominio 9 de ISO 27001:2013 Control de acceso y sus correspondientes objetivos de control como lo son:

- Requisitos de negocio para el control de accesos
- Gestión de acceso de usuarios
- Responsabilidades del usuario
- Control de acceso a sistemas y aplicaciones

Cada política se encuentra enfocada al mejoramiento de la seguridad informática respecto a los usuarios VPN, los cuales no cuentan con políticas específicas donde se detallen los lineamientos respecto a su creación y o uso.

Las políticas detalladas a continuación fueron expuestas a la Gerencia de la compañía B2B TIC S.A.S y se encuentran en proceso de revisión interna.

6.3.1 Políticas

Objetivos

Mostrar los elementos de la seguridad de la información para el obligatorio cumplimiento por parte de todo el personal y o contratistas de B2B TIC S.A.S.

Enunciado Políticas Seguridad de la Información.

En B2B TIC S.A.S la información es un activo fundamental para la prestación de su servicio. Por lo tanto, un compromiso primordial es el preservar la Confidencialidad, integridad y disponibilidad de la información de la compañía y de nuestros clientes, dando cumplimiento a los objetivos estratégicos, requisitos normativos, legales y contractuales aplicables promoviendo el desarrollo de estrategias de mejoras continua, es por ello que a continuación se relacionan las políticas diseñadas por la compañía respecto al dominio ISO 27001:2013 Control de Accesos.

1. Con el fin de garantizar la disponibilidad, integridad y confidencialidad de la información, B2B TIC S.A.S, asignara y empleara equipos que se encuentren únicamente sobre el dominio de Red de la compañía, estos deben ser utilizados por el personal asignado con su respectivo usuario y contraseña de red, para la solicitud se debe tener en cuenta el procedimiento 2020-10 Usuarios y para el correcto uso de contraseñas el procedimiento 2020-15

2. Todo equipo de cómputo debe tener antivirus actualizado y debe estar activo, el equipo de TIC es responsable de entregar el activo con el software antivirus actualizado y funcional, teniendo en cuenta la relación en el Acta de entrega.

3. Los usuarios que debido a sus roles tengan la necesidad de realizar conexiones desde redes externas a los recursos de la compañía únicamente lo deberán realizar por medio de conexiones seguras haciendo uso de VPN, las cuales deben estar aprobadas por parte de la Gerencia según procedimiento 2020-20 VPN.

Para realizar un seguimiento y monitoreo del correcto cumplimiento de las políticas establecidas, se utilizará el dominio 12 de ISO 27001:2013 correspondiente a Seguridad de las Operaciones y el objetivo de control de registro de actividad y supervisión, sobre el cual se realiza el correspondiente registro y gestión de eventos de actividad, por ello toda actividad realizada por los usuarios es debidamente registrada por los sistemas, por consiguiente cada uno de los usuarios debe conocer sus responsabilidades al hacer uso de cada uno de los sistemas de información accedidos mediante la utilización de la VPN, así como el adecuado uso de la red y accesos, ya que de evidenciar anomalías se realizará un llamado a descargos en caso de observar:

- Fallos de acceso repetitivos a la red o accesos con una cuenta distinta a la otorgada.
- Intentar o hacer uso de software de gestión remota como Team Viewer, Any Desk etc.
- Intentar acceder a dispositivos de red que no se encuentran autorizados.
- Intentar o realizar múltiples conexiones VPN.
- Elevado número de sesiones a servidores.
- Conexiones en horarios no laborales o que no sean habituales.
- Conexiones VPN de dispositivos que no sean propiedad de la compañía.
- Conexión de dispositivos que no cuenten con el antivirus actualizado y activo.

6.3.2 Procedimientos

2020-10 Usuarios

La creación y/o modificación de los usuarios del directorio activo están sujetos a autorización por parte de la Gerencia, por lo que cada uno de los jefes directos del personal deben realizar la solicitud formal vía correo al Gerente con copia a TIC, indicando en el asunto Autorización Nuevo Usuario o Autorización Modificación

Usuario según corresponda, incluyendo su firma en digital y la información correspondiente del personal Cedula, Nombre Completo, Cargo y Proyecto. Para la respectiva aprobación y ejecución se manejará tiempo estimado entre 12 - 24 horas tiempo durante el cual se dará respuesta vía correo con la información respectiva.

2020-15 Contraseñas

Las contraseñas asignadas a los usuarios nuevos son de un solo uso, por lo que el usuario al ingresar con los datos entregados es responsable de realizar el cambio de contraseña por una que cumpla los parámetros especificados de seguridad correspondientes al uso mínimo de 12 caracteres donde se utilicen símbolos, números, letras mayúsculas y minúsculas, además se cuenta con vencimiento de dicha contraseña cada 2 meses periodo en el cual se debe realizar la asignación de una nueva contraseña

2020-10 VPN

Cada uno de los jefes directos del personal deben realizar la solicitud formal vía correo al Gerente con copia a TIC, indicando en el asunto Autorización Nueva VPN o Autorización Modificación VPN según corresponda, incluyendo su firma en digital, la información correspondiente del personal como Cedula, Nombre Completo, Cargo, Proyecto, los permisos requeridos (dirección IP del servidor al que necesita acceder y puertos que requiere) y se debe incluir la asignación de un Token móvil. Para la respectiva aprobación y ejecución se manejará tiempo estimado entre 12 - 24 horas en el cual se dará respuesta por parte del área de TIC enviando el respectivo manual de instalación de la aplicación FortiClient y FortiToken, junto a un enlace con el instalador el cual tiene la preconfiguración correspondiente para que el usuario únicamente digite su usuario – contraseña y posteriormente el token asignado para obtener una conexión exitosa.

7 CONCLUSIONES

Al determinar el estado actual de la seguridad informática de la empresa B2B TIC SAS mediante el análisis de riesgo realizado con la ayuda de la metodología MAGERIT, se evidenció en la etapa de levantamiento de información que no se cuenta con una adecuada documentación de los activos y hojas de vida de estos, con lo cual no se tiene una cultura para el adecuado manejo de los activos frente a la seguridad informática, por lo que se deben generar procesos encaminados a su adecuado manejo a fin de que a mediano plazo se logren apalancar planes precisos para la continuidad del negocio.

En el análisis generado a los activos de la compañía B2B TIC S.A.S se evidencia una considerable cantidad de activos con riesgo alto, debido a que no se cuenta con una adecuada gestión de riesgo por la carencia de normas o políticas de seguridad informática, adicional a ello no se cuenta con concientización del personal para el adecuado uso de los recursos tecnológicos teniendo en cuenta las recomendaciones sobre la seguridad informática e información por falta de procesos de capacitación encaminados a la disminución de amenazas y riesgos asociados a dichos actores, los cuales son conocidos en el ámbito de la seguridad como el eslabón más débil.

Con la adición de una segunda capa de seguridad por medio de token para la conexión de los usuarios vía VPN y la integración del directorio activo vía LDAP al firewall, se garantiza la trazabilidad y monitoreo adecuado de la conexión y actividad de los diferentes usuarios que se encuentran ejerciendo sus funciones mediante la figura de teletrabajo, a fin de contar con un registro y control de estas evitando posibles suplantaciones.

Con la definición de políticas de seguridad basadas en el análisis de riesgo en donde se evidencia un número considerable de riesgos asociados a la confidencialidad y con la necesidad de contar con registro y monitoreo de conexiones. Se dan las

pautas para un adecuado manejo de los controles de usuario para el acceso VPN en la compañía B2B TIC SAS a fin de que se realice su análisis y difusión a cada uno de los colaboradores en pro de su cumplimiento.

8 RECOMENDACIONES

Debido al enfoque de la compañía B2B TIC S.A.S se recomienda realizar los procesos correspondientes para la definición e implementación de un sistema de gestión de la seguridad informática SGSI con base a la normativa ISO 27001:2013 a fin de mejorar los procesos internos, y de esta forma apalancar el crecimiento de la compañía.

Los miembros de la compañía deben recibir capacitación continua respecto al manejo y uso de los recursos informáticos, así como generar conciencia sobre la seguridad de la información y su importancia para la compañía B2B TIC S.A.S.

Se debe contar con análisis periódicos, con el fin de validar el cumplimiento de las políticas y controles establecidos, de esta forma evidenciar su efectividad o tomar las medidas correspondientes para su mejora continua.

BIBLIOGRAFÍA

Advisera Expert Solution LTD, ¿Qué es norma ISO 27001? (Disponible en internet): <https://advisera.com/27001academy/es/que-es-iso-27001>

APCER España, Sistemas de Gestión Ambiental. (Disponible en internet): <https://apcergroup.com/espana/index.php/es/newsroom/819/que-es-el-ciclo-pdca>

ÁLVAREZ BASALDÚA, Luis Daniel, "seguridad en informática (auditoría de sistemas)". (Disponible en internet): <http://www.bib.uia.mx/tesis/pdf/014663/014663.pdf>

BELLO,Claudia,"Manual de Seguridad en Redes". (Disponible en internet): <https://es.slideshare.net/csandovalrivera/manual-de-seguridad-en-redes>

BISOGNO, María Victoria, "Metodología para el Aseguramiento de Entornos Informatizados". (Disponible en internet): <http://materias.fi.uba.ar/7500/bisogno-degradoingenieriainformatica.pdf>

CISNEROS ESTUPIÑÁN, Mireya. Cómo elaborar trabajos de grado 2. Ed. Colombia: Ecoe Ediciones, 2012

CCIT y POLICIA, Tendencias cibercrimen Colombia 2019 - 2020. Bogotá: CCIT, 2019. (Disponible en internet): <https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf>

CHAVEZ, Nilda. Introducción A La Investigación Educativa.6 ed, Zulia: Editorial La Columna. 2007.

Diaz, A., et al. Implementación de un sistema de gestión de seguridad de la información (SGSI) en la comunidad nuestra señora de gracia, alineado tecnológicamente con la norma ISO 27001. (Disponible en internet): <http://www.konradlorenz.edu.co/images/stories/articulos/SGSI.pdf>

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Fortalecimiento de la Gestion TI en el estado. (Disponible en internet): <https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad>

El portal de ISO 27001 en español. Implantación. (Disponible en internet): <http://www.iso27000.es/sgsi_implantar.html>

_____, Sistemas de gestión de la seguridad de la información. (Disponible en internet): <http://www.iso27000.es/download/doc_sgsi_all.pdf>

HERNANDEZ, Sampieri. Metodología De La Investigación.6 ed, Mexico: Mc.Graw-Hill Interamericana Editores. 2006.

HERRERA PEREZ, Enrique. Tecnología y Redes de Transmisión de Datos. Limusa. México, 2003

IBARRA QUEVEDO, Raul. SERRANO LÓPEZ, Miguel Angel Calixto Garera y GONZALEZ, Carlos. Teoría de la información y encriptamiento de datos, México: Instituto Politécnico Nacional. 2010.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Trabajos escritos: presentación de tesis, trabajos de grado y otros trabajos de investigación. 6 ed. Bogotá D.C: INCONTEC, 2008 (NTC 1486)

_____. Documentación: Citas y notas de pie de página, 2 ed. Bogotá: ICONTEC, 1995. 7p. (NTC 1487).

INTERNATIONAL STANDARS ORGANIZATION – ISO. ISO/IEC 17799:2002. Tecnología de la Información. Código de buenas prácticas para la Gestión de la Seguridad de la Información.

_____.ISO/IEC 17799:2005. Tecnología de la Información –Técnicas de seguridad –Código para la práctica de la gestión de la seguridad de la información.

_____.ISO/IEC 27000.Tecnología de la Información – Técnicas de seguridad. Sistemas de Gestión de la Seguridad de La Información (SGSI).

LÓPEZ NEIRA, Agustín y RUIZ SPOHR, Javier. El portal de ISO 27001 en español, ISO 27000. (Disponible en internet): <http://www.iso27000.es/index.html>

MINISTERIO DEL TRABAJO, Libro blanco El abc del teletrabajo en Colombia. (Disponible en internet): <https://www.teletrabajo.gov.co/622/articles-8228_archivo_pdf_libro_blanco.pdf>

PNUD, ODS en Colombia; Los retos para 2030 Programa de las naciones unidas para el desarrollo PNUD. (Disponible en internet): <https://www.undp.org/content/dam/colombia/docs/ODS/undp_co_PUBL_julio_ODS_en_Colombia_los_retos_para_2030_ONU.pdf>

RISQUEZ, Gabriela. Metodología de la Investigación I: Manual teórico-práctico .2 ed, Caracas: URBE. 2002.

ANEXOS

Anexo 1. Controles Anexo A ISO 27001:2013 Gestión controles Acceso

A.9.1.1 Política de control de acceso
Se debe establecer, documentar y revisar con periodicidad una política de control de acceso, teniendo en cuenta los requisitos de la organización para los activos a su alcance. Las reglas, derechos y restricciones de control de acceso, junto con la profundidad de los controles utilizados, deben reflejar los riesgos de seguridad de la información de la organización.
A.9.1.2 Acceso a redes y servicios de red
El principio de acceso mínimo es el enfoque general para la protección, en lugar de acceso ilimitado y derechos de súper usuario sin una cuidadosa consideración. Como tales, los usuarios sólo deberían tener acceso a la red y a los servicios de red que necesitan usar o conocer para desarrollar su trabajo. Por lo tanto, la política debe abordar: Las redes y los servicios de red. Procedimientos de autorización para mostrar quién tiene acceso a qué y cuándo. Controles y procedimientos de gestión para evitar el acceso.
A.9.2.1 Registro de usuarios y anulación de registro
Es preciso implementar un proceso formal de registro y cancelación de registro de usuarios. Un buen proceso para la administración de ID de usuario incluye la posibilidad de asociar ID individuales a personas reales y limitar las ID de acceso compartido, que deben probarse y registrarse donde se haga.
A.9.2.2 Aprovisionamiento de acceso de usuario

Se debe implementar un proceso – simple y documentado – para asignar o revocar derechos de acceso para todos los tipos de usuarios, a todos los sistemas y servicios. El proceso de aprovisionamiento y revocación debe incluir: Autorización del propietario del sistema o servicio de información para el uso de estos activos. Verificar que el acceso otorgado sea relevante para el rol que se está realizando. Proteger contra el aprovisionamiento antes de que se complete la autorización. El acceso de los usuarios siempre debe estar dirigido por la organización y basado en los requisitos de esta.
A.9.2.3 Gestión de derechos de acceso privilegiado
Se trata de administrar niveles de acceso privilegiados, más altos y estrictos. La asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta, dados los derechos adicionales que generalmente se transmiten sobre los activos de información y los sistemas que los controlan.
A.9.2.4 Gestión de información secreta de autenticación de usuarios
La información secreta de autenticación es una puerta de acceso para llegar a activos valiosos. Por lo general, incluye contraseñas y claves de cifrado, por lo que debe controlarse mediante un proceso de gestión formal y debe ser mantenida en forma confidencial para el usuario. Esto generalmente está vinculado a contratos de trabajo y procesos disciplinarios, y obligaciones de proveedores.
A.9.2.5 Revisión de los derechos de acceso del usuario
Los propietarios de activos de a información deben revisar los derechos de acceso de los usuarios a intervalos regulares, tanto en torno al cambio individual – incorporación, cambio de rol y salida -, como a auditorías más amplias del acceso a los sistemas. Las autorizaciones para derechos de acceso privilegiado deben revisarse a intervalos más frecuentes, dada su naturaleza de mayor riesgo.
A.9.2.6 Eliminación o ajuste de los derechos de acceso

Los derechos de acceso de todos los empleados y usuarios externos a las instalaciones de procesamiento de información deben concluir al finalizar el vínculo laboral, el contrato o el acuerdo. Una buena política de salida garantizará que esto suceda.
A.9.3.1 Uso de información secreta de autenticación
Se trata simplemente de asegurar que los usuarios sigan políticos y asuman el compromiso de mantener confidencial cualquier información secreta de autenticación.
A.9.4.1 Restricción de acceso a la información
El acceso a la información y las funciones del sistema deben estar vinculadas a la política de control de acceso. Las consideraciones clave deben incluir: Control de acceso basado en roles. Niveles de acceso. Diseño de sistemas de menú, dentro de las aplicaciones. Leer, escribir, eliminar y ejecutar permisos. Limitación de la producción de información. Controles de acceso físicos y/o lógicos a aplicaciones, datos y sistemas sensibles. El auditor verificará que se hayan hecho consideraciones para limitar el acceso dentro de los sistemas y aplicaciones que soportan políticas de control de acceso, requisitos comerciales, niveles de riesgo y segregación de funciones.
A.9.4.2 Procedimientos de inicio seguro
El acceso a los sistemas y aplicaciones debe controlarse mediante un procedimiento de inicio de sesión seguro, para demostrar la identidad del usuario. Esto puede ir más allá del enfoque típico de contraseña de múltiples factores, biometría, tarjetas inteligentes y otros medios de cifrado en función del riesgo que se está considerando.
A.9.4.3 Sistema de gestión de contraseñas

El propósito de un sistema de administración de contraseñas es garantizar que estas sean de calidad, cumplan con el nivel requerido y se apliquen de manera consistente. Los sistemas de generación y gestión de contraseñas proporcionan una buena forma de centralizar el suministro de acceso, pero como sucede con cualquier control, deben implementarse cuidadosamente para garantizar niveles óptimos de seguridad y protección.
A.9.4.4 Uso de programas de utilidad privilegiada
Los programas informáticos que tienen la capacidad de anular controles del sistema y de las aplicaciones, aunque resulten muy útiles, deben ser gestionados con mucha atención. Ellos pueden ser un objetivo atractivo para atacantes maliciosos. El acceso a ellos debe restringirse al menor número de personas.
A.9.4.5 Control de acceso al código fuente del programa
El acceso al código fuente de los programas debe estar restringido, al igual que a los elementos asociados como diseños, especificaciones, planes de verificación y de validación. El código fuente de los programas informáticos, puede ser vulnerable a ataques si no está protegido en forma adecuada.

Fuente: https://www.escuelaeuropeaexcelencia.com/2019/09/como-gestionar-los-controles-de-acceso-segun-iso-27001, modificado por autor

Anexo 2. Ley 1273 de 2009

CAPITULO PRIMERO
De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos
Artículo 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO.

El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.
Artículo 269B. OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN.
El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.
Artículo 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS.
El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.
Artículo 269D. DAÑO INFORMÁTICO.
El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.
Artículo 269E. USO DE SOFTWARE MALICIOSO.

El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269F. VIOLACIÓN DE DATOS PERSONALES.

El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique p emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269G. SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES.

El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave. En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave. la pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

Artículo 269H. CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA.

Las penas imponibles de acuerdo con los artículos descritos en este título se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere: 1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros. 2. Por servidor público en ejercicio de sus funciones 3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este. 4. Revelando o dando a conocer el contenido de la información en perjuicio de otro. 5. Obteniendo provecho para si o para un tercero. 6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional. 7. Utilizando como instrumento a un tercero de buena fe. 8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.
CAPITULO SEGUNDO
De los atentados informáticos y otras infracciones
Artículo 2691. HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES.
El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.
Artículo 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS.
El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa. Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.

Fuente:http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492, modificado por autor

Anexo 3. Formato de Entrevista

FORMATO DE ENTREVISTA REPRESENTANTE LEGAL

Fecha: _____

Nombre de la empresa: _____

Nombre del entrevistado: _____

Cargo: _____

OBJETIVO:

Conocer el funcionamiento e infraestructura de la compañía B2B TIC SAS, junto con cada uno de los activos que intervienen en el desarrollo de las funciones de cada uno de los colaboradores de la compañía.

1. ¿En la compañía actualmente con cuantos empleados se cuenta?
   _____
2. ¿Qué área se encarga del soporte de la infraestructura tecnología de la compañía, cuantas personas la componen y quiénes son?
   _____
3. ¿Qué servicios como usuario consume estando en las oficinas de B2B TIC SAS?
   _____
4. ¿Conoce la cantidad y los equipos que intervienen para que sea posible consumir los servicios estando en las oficinas de la compañía B2B TIC SAS?
   _____
5. ¿En la actualidad conoce si se cuenta con documentación de los activos de la compañía actualizados a la fecha?
   _____
6. ¿Actualmente la compañía cuenta con un Sistema de gestión de la seguridad informática?
   _____
7. ¿Para los empleados de la compañía que tienen la posibilidad de realizar teletrabajo, de qué forma realizan el consumo de recursos de la compañía B2B TIC SAS y existe algún procedimiento-lineamiento para ello?
   _____

FORMATO DE ENTREVISTA PERSONAL DE TIC

Fecha: _____

Nombre de la empresa: _____

Nombre del entrevistado: _____

Cargo: _____

OBJETIVO:

Conocer en detalle el funcionamiento e infraestructura de la compañía B2B TIC SAS, junto con cada uno de los activos que intervienen en el desarrollo de las funciones de cada uno de los colaboradores de la compañía.

1. ¿En la actualidad se cuenta con alguna relación de asignación de equipos actualizada a la fecha, junto con la información de sistemas operativos y características de cada uno de ellos?
   _____
2. ¿Qué antivirus es utilizado por los equipos de cómputo entregados a los colaboradores de la compañía?
   _____
3. ¿Se cuenta con una topología lógica y física de la red de la compañía B2B TIC SAS?
   _____
4. ¿Qué proveedor de Internet, que ancho de banda y que equipo suministra el proveedor?
   _____
5. ¿Existe actualmente un Firewall sobre la red?
   _____
6. ¿Con cuántos Switch cuenta la compañía en su oficina y que referencia son?
   _____
7. ¿Qué equipo es utilizado para la red inalámbrica?
   _____
8. ¿Con cuantas impresoras se cuenta actualmente y que referencias son?
   _____
9. ¿En caso de que se presenten fallas eléctricas la compañía cuenta con alguna fuente de respaldo o UPS?
   _____

10. La compañía cuenta con servidores, ¿qué referencias?

_____

11. ¿La página web se encuentra alojada localmente o en un hosting, cuál?

_____

12. ¿Qué versión utilizan para el manejo de las bases de datos?

_____

13. ¿Se cuenta con un Servidor de archivos?

_____

14. ¿Se maneja un directorio activo para la compañía, que sistema operativo y versión maneja el servidor?

_____

15. ¿Qué equipo maneja el rol de servidor DHCP y DNS?

_____

16. ¿El servicio de correo de la compañía con quien se tiene contratado?

_____

Anexo 4. Tabla de clasificación de amenazas.

[N] Desastres naturales	**[I] De origen industrial**	**[E] Errores y fallos no intencionados**	**[A]Ataques deliberados**
[N.1] Fuego	[I.1] Fuego	[E.1] Errores de los usuarios	[A.4] Manipulación de la configuración
[N.2] Daños por agua	[I.2] Daños por agua	[E.2] Errores del administrador	[A.5] Suplantación de la identidad del usuario
[N.3] Desastres naturales	[I.3] Contaminación mecánica	[E.3] Errores de monitorización (log)	[A.6] Abuso de privilegios de acceso
	[I.4] Contaminación electromagnética	[E.4] Errores de configuración	[A.7] Uso no previsto
	[I.5] Avería de origen físico o lógico	[E.7] Deficiencias en la organización	[A.8] Difusión de software dañino
		[E.8] Difusión de software dañino	[A.9] [Re-]encaminamiento de mensajes

	[I.7] Condiciones inadecuadas de temperatura o humedad [I.8] Fallo de servicios de comunicaciones	[E.10] Errores de secuencia [E.14] Fugas de información [E.15] Alteración de la información	[A.11] Acceso no autorizado [A.12] Análisis de tráfico [A.13] Repudio [A.14] Interceptación de información (escucha)

[N] Desastres naturales	**[I] De origen industrial**	**[E] Errores y fallos no intencionados**	**[A]Ataques deliberados**
[N.1] Fuego [N.2] Daños por agua [N.3] Desastres naturales	[I.9] Interrupción de otros servicios o suministros esenciales [I.10]Degradación de los soportes de almacenamiento [I.11] Emanaciones electromagnéticas	[E.16] Introducción de falsa información [E.17]Degradación de la información [E.18] Destrucción de la información [E.19] Divulgación de información [E.20] Vulnerabilidades de los programas (software) [E.21] Errores de mantenimiento / actualización de programas (software) [E.23] Errores de mantenimiento / actualización de equipos (hardware)	[A.15] Modificación de información [A.16] Introducción de falsa información [A.17] Corrupción de la información [A.18] Destrucción de la información [A.19] Divulgación de información [A.22] Manipulación de programas [A.24] Denegación de servicio [A.25] Robo de equipos [A.26] Ataque destructivo [A.27] Ocupación enemiga
		[E.24] Caída del sistema por agotamiento de recursos [E.25] Pérdida de equipos [E.26] Indisponibilidad del personal	[A.28] Indisponibilidad del personal [A.29] Extorsión [A.30] Ingeniería social (picaresca)

Anexo 5. Manual activación FortiToken Mobile

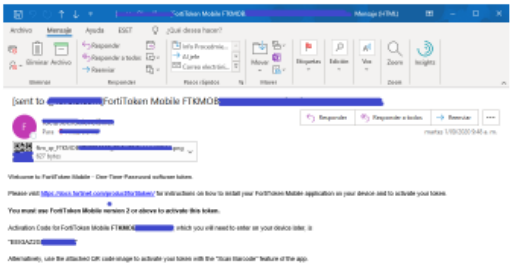
MANUAL ACTIVACION FORTITOKEN MOBILE

El presente documento tiene como fin detallar el paso a paso a llevar a cabo para la activación de un segundo factor de autenticación por parte del usuario, para posteriormente realizar la autenticación vía Vpn por medio de Forticlient a la red corporativa de la compañía B2B Tic.

Requerimientos previos:

- Mensaje de correo electrónico enviado por la plataforma al correo corporativo con la información de asignación de token móvil, código Qr y código de activación.

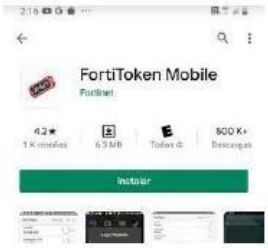
Imagen 1: Mensaje correo asignación FortiToken Mobile



Fuente: El autor

- Realizar la descarga e instalación de la aplicación FortiToken Mobile sobre dispositivo móvil Android desde Play Store.

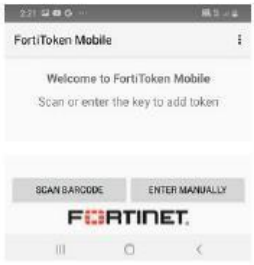
Imagen 2: Aplicación FortiToken Mobile en play store



Fuente: El autor

Una vez se cuenta con el correo de asignación del FortiToken Mobile y la aplicación Instalada, se procede a abrir la aplicación en donde se mostrarán 2 opciones correspondientes a Scan Barcode y Enter Manually.

Imagen 3: Opciones aplicación FortiToken Mobile

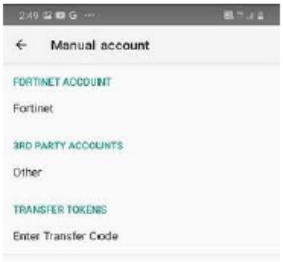


Fuente: El autor

Para facilitar el proceso seleccionar Scan Barcode y dar permisos para que la aplicación pueda hacer uso de la cámara, con ello sobre una computadora abrimos el adjunto del correo en donde podremos observar un código Qr, se escanea con la cámara y de forma automática realizara la activación del token , nos solicitara asignar una clave de 4 dígitos para para poder ingresar posteriormente a visualizar el token aleatorio asignado.

En el caso de que no se pueda escanear el código Qr darle en Enter Manually, seleccionar Fortinet e ingresar el correo electrónico corporativo y el Activation Code que está contenido en el mensaje de correo, una vez la aplicación haya validado la información solicitara la asignación de una clave de 4 dígitos para poder ingresar posteriormente a visualizar el token aleatorio asignado.

Imagen 4: Activación Manual FortiToken Mobile Selección Fortinet Account



Fuente: El autor

Imagen 5: Activación Manual FortiToken Mobile adición correo y Activation Code

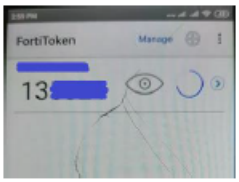
Fuente: El autor

Si el proceso ha sido exitoso nos mostrara una pantalla con un símbolo de un ojo con una raya en la mitad, el cual al tocarlo nos mostrara el token que ha sido asignado (6 dígitos) y en la parte derecha un círculo de estado que nos indica el tiempo de expiración del token.

Imagen 6: FortiToken Mobile Activo

Fuente: El autor

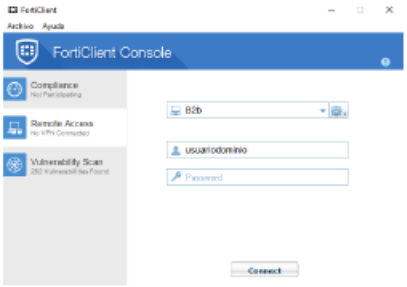
Imagen 7: FortiToken Mobile Activo con token Asignado



Fuente: El autor

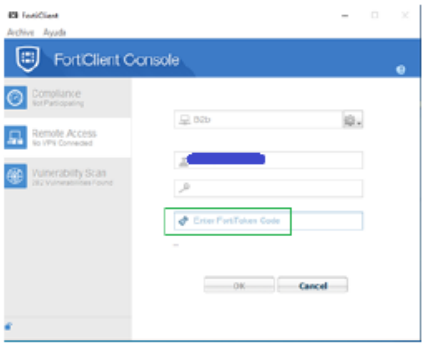
Una vez que tenemos el FortiToken Mobile activado y asignando los tokens podemos realizar el proceso de conexión con el cliente Vpn Forticlient con el correspondiente nombre de usuario y contraseña del dominio para que posteriormente nos pida ingresar un token generado por la aplicación y de esta forma lograr la conexión a la Vpn para consumir los recursos requeridos.

Imagen 7: Conexión Vpn Forticlient usuario y contraseña de dominio



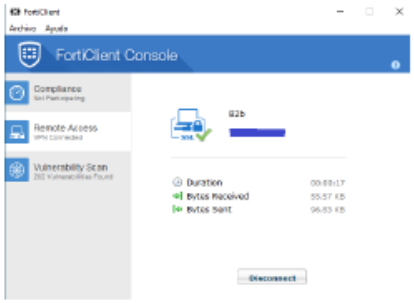
Fuente: El autor

Imagen 7: Ingreso de Token entregado por FortiToken Mobile sobre Forticlient



Fuente: El autor

Imagen 8: Autenticación correcta Vpn corporativa



Fuente: El autor

Control de Cambios	
Fecha de Creación	**Manual activación FortiToken Mobile**
2020, agosto 1	Versión 1
	Elaborado Por: Danilo Alfonso Arias Carreño