EVALUACIÓN DE LA SEGURIDAD DE LAS INFRAESTRUCTURAS TECNOLÓGICAS Y DE LA INFORMACIÓN EN UNA INSTITUCIÓN EDUCATIVA DE EDUCACIÓN MEDIA DE LA CIUDAD DE IBAGUÉ

YOVANNY ARCINIEGAS VILLARREAL

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
IBAGUE - TOLIMA
2022

EVALUACIÓN DE LA SEGURIDAD DE LAS INFRAESTRUCTURAS TECNOLÓGICAS Y DE LA INFORMACIÓN EN UNA INSTITUCIÓN EDUCATIVA DE EDUCACIÓN MEDIA DE LA CIUDAD DE IBAGUÉ

YOVANNY ARCINIEGAS VILLARREAL

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

YENNY STELLA NUÑEZ ALVAREZ
Tutora de Curso
JOEL CARROL VARGAS M.
Asesor

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGÍA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
IBAGUÉ - TOLIMA
2022

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad., Fecha sustentación

DEDICATORIA

Primeramente, a Dios que siempre me ha permitido alcanzar todos los objetivos propuestos, a mis padres, mis hijas y mi bella esposa que siempre ha estado pendiente y presta para apoyar todos mis procesos de enriquecimiento personal, todos ellos que siempre me han apoyado con paciencia, dedicación, buenos consejos y abrazos de alegría por el interés de adquirir conocimiento día a día, agradezco con gran amor todo lo que hacen.

AGRADECIMIENTOS

Agradecimiento inmenso a Dios por permitirme la salud para alcanzar un objetivo más en la vida, al equipo de trabajo de la UNAD, porque con su tarea de educar fortalecen competencias para la vida laboral, por otro lado, a cada uno de los tutores y asesores que, con su profesionalismo, sentido de pertenencia y paciencia me acompañaron y orientaron efectivamente en el proceso.

CONTENIDO

pág.

INTRODUCCIÓN *15*

1. DEFINICIÓN DEL PROBLEMA *16*

1.1 ANTECEDENTES DEL PROBLEMA **16**

1.2 FORMULACIÓN DEL PROBLEMA **17**

2 JUSTIFICACIÓN *18*

3 OBJETIVOS *19*

3.1 OBJETIVOS GENERAL **19**

3.2 OBJETIVOS ESPECÍFICOS **19**

4 MARCO REFERENCIAL *20*

4.1 MARCO TEÓRICO **20**

4.1.1 Panorama De Seguridad 21

4.2 MARCO CONCEPTUAL **21**

4.2.1 Seguridad de la Información 21

4.2.2 Políticas de Seguridad 22

4.2.3 Infraestructura Tecnológica 22

4.2.4 Mecanismos de Endurecimiento de Seguridad 22

4.2.5 Normatividad 22

4.3 MARCO HISTÓRICO **23**

4.4 MARCO LEGAL **23**

5 DISEÑO METODOLÓGICO *25*

5.1 TIPO DE INVESTIGACIÓN Y ALCANCE **25**

5.2 DISEÑO DE LA INVESTIGACIÓN **26**

5.3 MÉTODO PARA LA BUSQUEDA INFORMACIÓN **26**

6 **MINIMAS MEDIDAS DE SEGURIDAD DE LAS INFRAESTRUCTURAS** **27**

6.1 PROCEDIMIENTOS DE SEGURIDAD **28**

6.1.1 Copias de Seguridad 28

6.1.2 Almacenamiento en la nube 28

6.1.3 Control de Acceso a información sensible 29

6.1.4 Creación de contraseñas seguras 29

6.1.5 Protección del correo electrónico 30
6.1.6 Uso de software DLP 30
6.1.7 Monitorización y respuesta inmediata 31

7 ACCIONES PARA ENDURECER LA SEGURIDAD DE LA INFORMACION 32

7.1 EL ENDURECIMIENTO 33

7.2 Expertos en el proceso de endurecimiento 34
7.2.1 Líder del proyecto infraestructura, ... 34
7.2.2 Analista de sistemas 34
7.2.3 Diseñador 34
7.2.4 Responsable de Configuración y Pruebas 34

7.3 ENDURECIMIENTO DE SOFTWARE 35
7.3.1 IDS/IPS Y FUNCIONAMIENTO 35
7.3.2 Firewall Virtualizado 36

7.4 ENDURECIMIENTO DE HARDWARE 36
7.4.1 Firewall físico 36
7.4.2 Router 38
7.4.3 Switch. 39
7.4.4 Servidores 41

7.5 ENDURECIMIENTO DE CONFIGURACION 42
7.5.1 Implementación DMZ 42

8 DISEÑO TOPOLOGIA DE RED CON MECANISMOS DE ENDURECIMIENTO *43*

8.1 La arquitectura de los dispositivos a implantar 45

8.2 Administración de la Infraestructura Tecnológica. 49

9 CONCLUSIONES 50

10 RECOMENDACIONES 51

11 BIBLIOGRAFÍA 52

LISTA DE TABLAS

pág.

Tabla 1. Infraestructura del Centro Educativo 31

LISTA DE FIGURAS

Pág.

Figura 1: Como ocurren los ataques 20
Figura 2. Pilares de la información 28
Figura 3. IDS-IPS series 1100 Forcepoint 34
Figura 4. Firewall virtualizado Forcepoint. 35
Figura 5. Firewall NGFW Forcepoint 36
Figura 6. Router Gigabit multi-WAN VPN TWG-431BR (Version v1.0R) 37
Figura 7, ZyXEL GS1900-24 L2 24p Gigabit – Switch 38
Figura 8. Servidor en rack PowerEdge R250 39
Figura 9. Topología con mecanismo de endurecimiento de la Infraestructura 41
Figura 10. Arquitectura de los IDS/IPS 42
Figura 11. Arquitectura de los Router y Switch en el modelo OSI 42
Figura 12. Arquitectura cliente – servidor 44
Figura 13. Arquitectura Firewall NGFW Forcepoint 45
Figura 14. Arquitectura DZM 46

LISTA DE CUADROS

pág.

Cuadro 1. Especificaciones Firewall NGFW series 1100 37
Cuadro 2. Características Firewall NGFW series 1100 37
Cuadro 3. Especificaciones Router Gigabit multi-WAN VPN TWG-431BR 38
Cuadro 4. Detalles modelo ZyXEL GS1900-24 L2 24p Gigabit – Switch 39
Cuadro 5. Características de ZyXEL GS1900-24 39
Cuadro 6. Especificaciones técnicas 40

GLOSARIO

Seguridad informática

Estrategias, medidas, buenas prácticas y herramientas destinada a la protección de la información y de los activos informáticos de cualquier ataque de la ciberdelincuencia, en esta tarea está presente las personas.

Infraestructuras tecnológicas,

En un conjunto de componentes o activos que trabajan integralmente para generar procesos u operaciones en una institución u organización.

Información

Son datos debidamente organizados que contienen hechos, asuntos de conocimiento para personas, tienen contenido que puede ser comunicado o trasmitido.

Redes

Es un conjunto de dispositivos intercomunicados entre sí mediante cables o inalámbricamente para trasporte de datos, comparten información de interés.

Topología

Es un mapa que sirve para identificar la ubicación de dispositivos o componentes de una red para la actividad de intercambiar datos. Es la forma de diseño para fijar como está conformada la red en la parte física o lógica.

Activo

Es todo componente que hace parte de una infraestructura y que altamente valioso para objeto social que desarrolla una institución u organización.

Riesgo

Se presenta como la eventualidad u oportunidad para que la infraestructura tecnológica sufra un quebranto de seguridad que trae problemas económicos.

Amenaza

Es aquella actividad que puede agredir un sistema informático y causar daño a la información que se maneja.

Vulnerabilidades

Es conocida como aquella debilidad en la seguridad de una infraestructura colocando el activo de la información en condiciones de riesgo, esta puede facilitar que el ataque de un delincuente informático se fructífero.

Impacto

Es el resultado o consecuencia generada por una intervención.

Firewall

Es un componente físico o lógico que realiza la gran tarea de controlar el acceso a una un dispositivo o red con el propósito de brindar seguridad.

Proteger

Toda actividad tendiente para defender de un ataque a una infraestructura tecnológica y la información de una agresión informática.

Políticas de seguridad

Son tocas aquellas medidas que se ejecutan para prevenir, proteger, afrontar y minimizar asuntos de seguridad en una Institución.

Ataque dirigido

Conocido por ser aquellos que están dirigidos a sustraer datos que controlan el acceso a dispositivos que contiene información. Existe toda una planificación de un ciberdelincuente, tiene un objetivo específico o se aprovecha de una vulnerabilidad.

RESUMEN

Las infraestructuras tecnológicas y la información son activos valiosos los cuales demandan de una cuidadosa, ardua e incansable tarea para su protección y para el debido funcionamiento en cualquier institución de educación, de ahí que seguir las políticas y estrategias de seguridad se convierte en una necesidad a la cual hay que prestar demasiada atención y cuidado para evitar situaciones que puedan afectar gravemente la información y el desarrollo normal de la función fundamental de educar. A medida que avanza el desarrollo tecnológico también llega con ella las ciberamenazas, la situación amerita toda la atención para abordar de manera organizada este tema tan serio relacionado con la seguridad informática, así que proteger la infraestructura tecnológica y la información es adelantar también los procesos para proteger de igual forma la institución de amenazas que puedan afectar el activo tan valioso de la información. Contar con una adecuada infraestructura es primordial y exigente, esa labor incluye sin duda algunas estrategias de seguridad y de fortalecimiento de los activos que la conforman, la aplicación de mecanismos de endurecimiento permite que la institución de educación media cumpla con su objetivo fundamental y se mantenga a la vanguardia con la seguridad que debe tener la infraestructura y la información.

Descriptores: Infraestructuras, información, activos, políticas y estrategias de seguridad.

ABSTRACT

Technological infrastructures and information are valuable assets which demand care to, arduous and tireless task for their protection and for the proper functioning in any educational institution, hence following security policies and strategies becomes a necessity to which we must pay too much attention and care to avoid situations that can seriously affect information and the normal development of the fundamental function of educating. As technological development progresses, cyberthreats also come with it, the situation deserves all the attention to address in an organized manner this serious issue related to computer security, so protecting the technological infrastructure and information is also advancing the processes to Protect the institution from threats that may affect the valuable asset of information. Having an adequate infrastructure is essential and demanding, this work undoubtedly includes security strategies and strengthening of the assets that make it up, the application of hardening mechanisms allows the secondary education institution to fulfill its fundamental objective and remain at the forefront with the security it must have. infrastructure and information.

Descriptors: Security infrastructures, information, assets, policies and strategies.

INTRODUCCIÓN

Con la llegada de la tecnología también han ido apareciendo diferentes acontecimientos de inseguridad informática que crean la necesidad de implementar la integralidad de componentes físicos y tangibles en las infraestructuras tecnológicas que desarrollan funciones importantes y que están plenamente relacionadas con la información que maneja toda entidad, organización e institución.

Se convierte entonces una esencialidad que las infraestructuras tecnológicas mantengan la disponibilidad de los servicios[1] y las funciones a través de sus componentes debe darse de manera segura para que el desarrollo del objetivo nunca pare, la infraestructura debe estar en condiciones óptimas de funcionalidad permanente, ofreciendo un servicio libre de incidencias que afecten la labor de las instituciones.

De ahí que se presenta la exigencia de conocer el estado de la infraestructura mediante la evaluación periódica con el propósito de aplicar mecanismos de endurecimiento que permitan que el trabajo de la infraestructura esté a la vanguardia de seguridad y especialmente de la seguridad de la información.

Siendo las cosas de esta manera, el presente trabajo está orientado a la evaluación de la seguridad de las infraestructuras tecnológicas y de la información en una institución educativa de educación media de la ciudad de Ibagué, conociendo su verdadero estado para poder identificar lo que debe adecuarse con la implementación de acciones que conlleven al fortalecimiento de las medidas correspondiente para la protección de la tarea de la institución, la infraestructura, y la información.

La simple existencia de la infraestructura, su funcionalidad no es sinónimo de seguridad, de ahí que la importancia de su fortalecimiento mediante la actualización de activos o componentes de vanguardia en seguridad no debe dejarse de lado, pues estos más una administración exigente de la infraestructura hace que siempre esté disponible para los procesos requeridos por la institución, si hacemos una comparativa de las medidas de seguridad físicas e intangibles aplicadas hace siete años sorprenden su gran evolución, está evolución producida por los ataques realizados, los avances tecnológicos demandan también estar actualizados de herramientas que apoyen la tarea de seguridad para hacer frente firme a los ataques perpetuados por ciberdelincuentes.

[1] QUINTERO MARTINEZ, Manuel, I. y TOVAR BALDERAS, Sergio A. TiES Revista de Tecnología e Innovación en Educación Superior, 2021., p,3.

1. DEFINICIÓN DEL PROBLEMA

Son demasiados los pronunciamientos del Estado en lo concerniente con la seguridad de la información y el fortalecimiento de las infraestructuras tecnológicas en la educación, por tanto, se presenta la necesidad de abordar este estudio relacionado con el ajuste del fortalecimiento de seguridad de las Infraestructuras Tecnológicas y de la Información en una Institución Educativa de Educación Media de La Ciudad de Ibagué.

En el complejo tema de los avances tecnológicos y la implementación de infraestructuras tecnológicas fortalecidas de medidas de seguridad que logren la protección de la información son el eje central de toda institución de educación, una infraestructura que cuente con las políticas de seguridad proporciona un efectivo mecanismo para lograr el nivel de autonomía alineada con la necesidad de la educación. La seguridad comienza con la gestión continua de estrategias para minimizar los riesgos y amenazas dirigidas por los delincuentes informáticos, evaluar los riesgos permite la comprobación real de su estado actual, para realizar los ajustes correspondientes para adecuarla al nivel de seguridad requerido que permita de tal manera salvaguardar los procesos que se adelantan en una Institución de educación media.

La información y tecnología representan un activo valioso para las Instituciones, y contar con una infraestructura efectiva que abarque los parámetros necesarios en la satisfacción de la exigencia informática, la cual presenta una especial función de preparar a los estudiantes, además del cumplimiento de la función de la institución puede organizar y almacenar[2] la información con la garantía de disponibilidad, confiabilidad e integridad de los datos. Encontramos en este momento de abordar el estudio muchos interrogantes ¿Cuál es el estado actual de la infraestructura tecnológica?, ¿Qué medidas de seguridad utiliza para proteger la información?, ¿Cuenta la Institución de educación media con políticas de seguridad efectivas?

1.1 ANTECEDENTES DEL PROBLEMA

En los últimos tiempos, debido a los avances vertiginosos de la tecnología han llegado nuevos desafíos que afrontar por parte de los Estados y los distintos sectores, exigencia de la implementación de políticas y estrategias serias para hacer frente, Colombia no es la excepción, tomar las medidas acordes en los últimos años por los organismos y entidades que hacen parte del sector público y privado

[2] ROSALES MONTALBAN, Eduardo, otros... Diseño de un Sistema de Gestión de Seguridad de la Información para el Proceso de Gestión de la Infraestructura Tecnológica de Instituciones académicas Basado en Magerit, 2019.

utilizando los instrumentos jurídicos que permitan al país estar al día en la seguridad cibernética.

Como lo presenta Tecnósfera (2014):

En Colombia una gran cantidad de personas estuvieron comprometidas en calidad de victimarias de la criminalidad tecnológica, Estos delitos en el año 2013 tuvo cuantiosos daños económicos de 874 mil millones de pesos según la firma Norton.

Según la Cámara Colombiana de Informática y Telecomunicaciones (CCIT):

"El cibercrimen durante el 2021 ha mantenido la tendencia observada desde el 2019, con un incremento continuo, que para el actual periodo en análisis ya alcanza un 35% respecto al 2020. Con más de 20.502 noticias criminales registradas en el ecosistema de ciberseguridad, frente a 15.107 reseñadas en el mismo periodo de tiempo durante el 2020 (enero-mayo); los ataques de phishing, el secuestro de información o ransomware y la filtración o fuga de datos personales se mantienen en primer lugar como las tendencias más frecuentes[3]".

La CCIT, "realiza un análisis en su orden de primer lugar, de 5.734 noticias delincuenciales informáticas en Colombia, sobre el quebrantamiento de datos personales en el 2020. Segundo Lugar, Suplantación De Sitios Web Para Capturas Datos Personales con 2.473 casos puestos a conocimiento de la Fiscalía en el 2020. Tercer Lugar, por el Acceso Abusivo A Sistema Informático con 3.326 denuncias instauradas en el 2021".

Las amenazas actuales de los delincuentes informáticos se han vuelto especialmente maliciosas y avanzadas en estos últimos meses, aprovechando las vulnerabilidades expuestas por la masiva utilización de los sistemas informáticos por la situación de pandemia, que conlleva a cometer errores relacionado a la omisión de la aplicación de las buenas prácticas en los aconteceres diarios en el manejo de los dispositivos tecnológicos.

1.2 FORMULACIÓN DEL PROBLEMA

Evaluación de la Seguridad de las Infraestructuras Tecnológicas y de la Información en una Institución Educativa de Educación Media de la Ciudad de Ibagué.

[3] CCIT. (2021). "Evaluación, Retos y Amenazas de Ciberseguridad", 2021.

2 JUSTIFICACIÓN

Desde hace algunas décadas, la información e infraestructuras tecnológicas en conjunto han tomado el valor de activo valioso para cualquier Institución, en Colombia son muchas las empresas que han sufrido ataques cibernéticos por parte de delincuentes informáticos, desde esos momentos nace la necesidad de adelantar actividades adecuadas para minimizar los riesgos en términos de seguridad informática. Si hablamos a nivel internacional estaríamos frente a cantidad de casos que se han registrado por parte de los ciberdelincuentes[4].

En Colombia el sector público y como el privado han sido objeto de casos de fuga de información, la vulnerabilidad se ha presentado en los sistemas informáticos y redes lo cual ha dejado como resultado pérdidas económicas y al buen nombre, ha llegado inclusive al cierre de algunas entidades. Para contrarrestar todas estas conductas desplegadas por los ciberdelincuentes el Estado Colombiano expide Ley 1273 de 2009 la cual modifica la Ley Penal 599 de 2000, la cual describe tipos penales de conductas relacionadas con la sustracción de información mediante el acceso no permitido a equipos informáticos; de igual manera documentos de planes estratégicos de seguridad informática.

Son variadas las modalidades y estrategias que usan los ciberdelincuentes para atacar y colocar en riesgo el activo de la información, por tanto no es desbordado en este estudio adelantar el proceso de evaluación de riesgos de la infraestructura tecnológica de una institución educativa de educación media de la ciudad de Ibagué, porque con ello se está protegiendo la información, mediante el uso de las mismas herramientas tecnológicas se puede preservar un activo valioso y sobre todo la función tan importante de educar que se desarrolla en la mencionada Institución.

[4] Ing. ROMERO ROA, Luis, F. “Seguridad Informática en Colombia. Universidad Piloto de Colombia. Bogotá D.C”, 2015.

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Evaluar el proceso de la seguridad de la información a través de las infraestructuras tecnológicas.

3.2 OBJETIVOS ESPECÍFICOS

• Identificar las mínimas medidas de seguridad de las infraestructuras que deben tener las instituciones de educación media de acuerdo con la normatividad y referencias académicas en Colombia.

• Describir las acciones para endurecer la seguridad de la información en las instituciones de educación media en Colombia.

• Esquematizar una topología de red que aplique los mecanismos de endurecimiento de la infraestructura del centro educativo.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

De gran importancia se presenta el proceso de protección de los recursos con los que cuenta una Institución para desarrollar su actividad fundamental, los dispositivos que conforman las infraestructuras generan acceso a los usuarios quienes diariamente manejan grandes cantidades de datos los cuales son llamativos a las actividades ilegales de los atacantes. Las vulnerabilidades y ataques a la infraestructura se presentan también por contar con activos físicos y tangibles obsoletos o desactualizados, en el caso del cortafuegos realiza una tarea importante de seguridad de primera línea de defensa en una red, si este no está a la vanguardia sería propicia la vulnerabilidad para ser aprovechada por el atacante cibernético.[5]

Colombia al presentar debilidades en la seguridad de sus infraestructuras tecnológicas, toma las medidas necesarias tendientes a minimizar y contrarrestar el riesgo que se presenta actualmente, adoptando las políticas, estrategias a través de su MINTIC, generando Plan Estratégico de Tecnologías de Información (PETI), y documentos CONPES para la protección de la información[6].

Proceso de evaluación necesario ejecutarlo para conocer el estado en que se encuentra los activos que conforman la infraestructura tecnológica y la información, con la cual se puede evidenciar los riesgos, vulnerabilidades, y las medidas de seguridad a tomar para su protección efectiva, además de crear conciencia y cultura de sensibilización para la prevención de incidentes de seguridad y evitar resultados catastróficos en una institución.

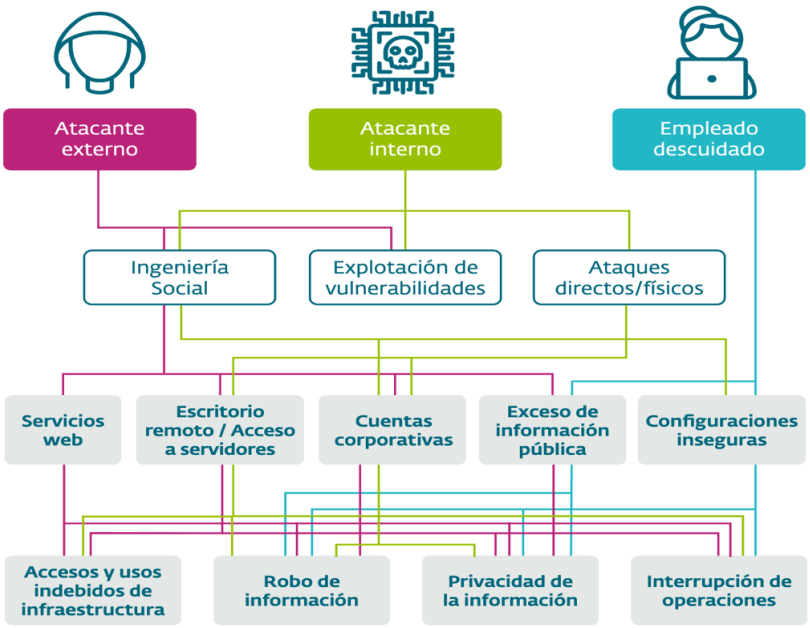
En este sentido, González (2011) plantea que la Seguridad Informática, “es la disciplina que se encargaría de las implementaciones técnicas de la protección de la información, el despliegue de las tecnologías antivirus, firewalls, detección de intrusos, detección de anomalías, correlación de eventos, atención de incidentes, entre otros elementos, que articulados con prácticas de gobierno de tecnología de información establecen la forma de actuar y asegurar las situaciones de fallas parciales o totales, cuando la información es el activo que se encuentra en riesgo". (Gonzalez,2011)”[7]

[5] HewlettPackard Enterprise. Seguridad en Infraestructura, 2022.
[6] GONZALEZ HERNANDEZ, Mauricio. “Actualidad de Colombia en Seguridad Informática. Universidad Piloto de Colombia”, 2021.
[7] GONZALEZ. (2011). Citado por FIGUEROA SUAREZ, Juan, A, otros... “La seguridad informática y la Seguridad de la información”, 2017.

4.1.1 Panorama De Seguridad

No es para menos la preocupación en Colombia, por la cantidad de casos que se han presentado en los últimos años de fuga de información y de dato personales cada día en crecimiento, problemática que afecta al sector público como el privado. La toma de medidas para garantizar altos niveles de seguridad no se hace de esperar para los sectores, implementar dinámicas y concientización para la protección de datos conlleva retos que hay que afrontar.

Figura 1: Como ocurren los ataques.



Fuente: ESET. Security Report. Latinoamérica 2020. [en línea]. [Recuperado 16 de octubre 2022]. Disponible en: https://www.welivesecurity.com/wp-content/uploads/2020/08/ESET-Security-Report-LATAM_2020.pdf

4.2 MARCO CONCEPTUAL

Trata de una sistemática síntesis de la terminología empleada dentro del presente marco de referencia y que se utiliza en el transcurso del desarrollo del proyecto.

4.2.1 Seguridad de la Información

Es el estado de ausencia de riesgo, bienestar, y vulnerabilidades. Se mantiene a través de los procesos de evaluar y gestionar los riesgos a los que se encuentra la

información. Las medidas para mantener un sistema seguro siempre están acompañadas de procedimientos sobre control de riesgos, con acciones necesarias para evitar o prevenirlo.

4.2.2 Políticas de Seguridad

Son las orientaciones e instrucciones para manejar de manera organizada los asuntos relacionados con la seguridad y conforman los planes a tener en cuenta para implantar las medidas de prevención, protección y hacer frente a los ataques para minimizarlos.

Las políticas por lo general van acompañadas de indicaciones sistemáticas de procedimientos a seguir por parte de los expertos en seguridad informática o encargados de la infraestructura tecnológica.

4.2.3 Infraestructura Tecnológica

Está plenamente relacionada con los componentes físicos e intangibles que la componen, con el propósito de realizar la transmisión de datos que interesan a una organización o institución en el cumplimiento de sus objetivos.

Los componentes que hacen parte de la infraestructura son activos tecnológicos valiosos de hardware software, que realizan tareas de gestión de datos de salida y entrada y donde participa activamente la intermediación de personas.

Topologías de Red

Es el diseño de la cadena de comunicación física o inalámbrica que compone una red de dispositivos que se conectan entre sí para la transmisión de datos de interés.

4.2.4 Mecanismos de Endurecimiento de Seguridad

Son todos aquellos elementos, dispositivos, y prácticas para minimizar vulnerabilidades de una infraestructura, siendo necesarias para el fortalecimiento de la seguridad. Se presenta como la necesidad de la actualización de vanguardia de los equipos que la componen y que demanda la observancia de estos mecanismos para la función efectiva de proteger.

4.2.5 Normatividad

En sentido estricto, Es el compendió jurídico del cual hace uso el Estado para propender por la seguridad de las infraestructuras tecnológicas y de la información.

4.3 MARCO HISTÓRICO

Desde los primeros pasos de la raza humana en la tierra la información ha estado presente, el hombre para representar sus hábitos, costumbres, cultura, medios utilizados por él y por otras personas a través del tiempo, esta información valiosa fue tomando importancia y se fue ampliando con registros de objetos preciosos, pinturas magnificas entre otros, su acceso solo lo tenían quienes estuviesen autorizados para su interpretación; las civilizaciones egipcias ejemplo de estos primeros sistemas de escrituras basados en jeroglíficos hace millones de años. Hoy, la información sigue ocupando un alto valor para la sociedad y para las organizaciones especialmente en loque tiene que ver a la toma de decisiones según sus funciones.

La definida sociedad de la información, es un tema amplio que ha sido comentado y tratado de manera detallada, y se centra en su conceptualización donde las tecnologías juegan papel importante facilitando crear, administrar, manipular la información por jugar transcendental papel en la tareas que desarrolla la sociedad, son muchos los países que han participado especialmente en el orden la industria con el punto de orientación de desarrollo, progreso de la sociedad, de la gestión efectiva de la productividad y demás fines que favorecen a la comunidad de manera global.

La Información como elemento fundamental en la sociedad y como activo valioso en las Instituciones debe contar con entera disponibilidad para la decisión y desarrollo de los objetivos corporativos y a su vez su adecuado manejo brinda confianza y permanencia al cliente. Ahí se presenta la necesidad de ser protegida, Colombia se ha unido con otros Estados legislativamente para la protección de los dispositivos tecnológicos y de la información, trabajando en equipo y ejecutando políticas y estrategias para el fortalecimiento de la seguridad que favorezca la infraestructura y el activo valioso en su integridad, confidencialidad y disponibilidad para su uso sin contratiempos que puedan generar menoscabos que afecten tanto económicamente, y servicios u objeto social de la entidad.

4.4 MARCO LEGAL

El avance tecnológico no es ajeno al derecho, impone grandes retos para afrontar desde óptica de la legislación nacional, internacional, el derecho comparado, la autonomía de la voluntad privada y las mejores prácticas. El Estado Colombiano en su propósito de protección de infraestructuras tecnológicas y de la información expidiendo normas jurídicas que respondan a los problemas que surgen del uso cotidiano de la tecnología.

- Carta política de 1991 de Colombia artículos 15 y 20.

- Ley 23 de 1982, Sobre derechos de autor

- Ley 527 de 1999, Por medio de la cual se define y se reglamenta el acceso y el uso de los mensajes de datos.

- Decreto 1747 de 2000, por el cual se reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales.

- Ley 1273 de 2009. Establece la protección de la información y de los datos.

- Documento CONPES 3975. Política Nacional para la Transformación Digital e Inteligencia Artificial, del 8 de noviembre de 2019. El Consejo Nacional de Política Económica y social (CONPES). Colombia. Departamento Nacional de Planeación.

- Documento CONPES 3995. Política Nacional de Confianza y Seguridad Digital. del 1 de julio de 2020. El Consejo Nacional de Política Económica y social (CONPES). Colombia. Departamento Nacional de Planeación.

5 DISEÑO METODOLÓGICO

Como se expuso al comienzo con la introducción, este trabajo orientado a la seguridad de las infraestructuras tecnológicas y de la información en una institución educativa de educación media de la ciudad de Ibagué. La infraestructura es de vital importancia que mantengan la disponibilidad de sus servicios para que los procesos corporativos no se detengan.

La evaluación de las condiciones en que se encuentra la infraestructura tecnológica identificando las mínimas medidas de seguridad con las que cuenta, en lo relacionado con sus componentes y configuración de los activos físicos y lógicos para la protección de la información como activo valioso observando la normatividad y asuntos académicos en Colombia.

La descripción sistemática de acciones para el endurecimiento de la red para proteger los datos es la base esencial para tener en cuenta, con el propósito de lograr el nivel apropiado para la minimización de las amenazas que puedan afectar gravemente los pilares que la componen de integridad, confidencialidad y disponibilidad.

El diseño de topología de red, donde se vea reflejada la configuración de los dispositivos que componen la infraestructura con mecanismos efectivos que conlleven al funcionamiento fortalecido para evitar incidencias que la puedan afectar gravemente y por ende a la institución.

5.1 TIPO DE INVESTIGACIÓN Y ALCANCE

Se procede para lograr el desarrollo de este trabajo investigativo aplicar la metodología documental, la ofrece una amplia opción de análisis y estudio de obras, documentos físicos y digitales, y demás bibliografías atinentes al caso, sin desatender la legislación sobre los derechos de autor , esto permite de tal forma el juicioso estudio de las diferentes fuentes de información relacionada con la infraestructura tecnológica y la protección del activo valioso de la información en las instituciones Colombianas especialmente en lo observable a las estrategias de seguridad tecnológicas para hacer frente a las amenazas presentadas por los ciberdelincuentes que tanto pueden afectar en este caso una Institución educativa de educación media de la ciudad de Ibagué.

5.2 DISEÑO DE LA INVESTIGACIÓN

La investigación diseño no experimental, según lo considerado por Hernández, Fernández y Baptista, 2014, definen este tipo como "la investigación que se realiza sin manipular deliberadamente variables. Es decir, se trata de estudios en los que no hacemos variar en forma intencional las variables independientes para ver su efecto sobre otras variables. Lo que hacemos en la investigación no experimental es observar fenómenos tal como se dan en su contexto natural, para analizarlos[8]".

"Los diseños transaccionales o transversales recolectan datos en un solo momento, en un tiempo único. Su propósito normalmente es: 1. Describir variables en un grupo de casos (muestra o población), o bien, determinar cuál es el nivel o modalidad de las variables en un momento dado. 2. Evaluar una situación, comunidad, evento, fenómeno o contexto en un punto del tiempo[9]" (Hernández y Mendoza 2018)

5.3 MÉTODO PARA LA BUSQUEDA INFORMACIÓN

Según Alfonso (1995), "la investigación documental es un procedimiento científico, un proceso sistemático de indagación, recolección, organización, análisis e interpretación de información o datos en torno a un determinado tema. Al igual que otros tipos de investigación, éste es conducente a la construcción de conocimientos."

Comprende la investigación documental, fuentes impresas y digitales que abarcan libros, revistas sobre avances tecnológicos, manuales, tesis, monografías y demás documentos que juegan papel importante y que son útiles y de vital importancia para el desarrollo de la investigación y que hoy son muy asequibles en internet.

[8] HERNANDEZ SAMPIERI, Roberto, otros… Metodología de la Investigación. Sexta Edición, Editorial Mexicana, Reg. Número 736 México D.F, 2014 p, 152.
[9] HERNANDEZ SAMPIERI, Roberto, otros… Metodología de la Investigación. Primera Edición. Editorial Mexicana Reg. No. 736. México D.F, 2018". p,215.

6 MINIMAS MEDIDAS DE SEGURIDAD DE LAS INFRAESTRUCTURAS

La seguridad de una infraestructura podemos compararla como la seguridad que normalmente tenemos en el hogar, las diferencias se encuentran con las características técnicas aplicables a los sistemas, la actividad diaria de proteger bienes valiosos de grandes riesgos y vulnerabilidades que mediante la ejecución de medidas configurables se presenta compleja. Sin embargo, el fin esencial es el mismo el de brindar protección a la infraestructura de esa Institución que cumple su función mediante la utilización de un sistema tecnológico.

Las mínimas medidas de seguridad deberían ser suficientes para la seguridad de la infraestructura, no tendría por qué presentarse incidencia alguna de riesgo de seguridad, debería funcionar sin menoscabo alguno, pero sucede lo contrario, como en cualquier contexto de la sociedad, siempre hay un riesgo en cualquier actividad, y ahí es donde nace la obligación de mantener a nivel actual la medida para contrarrestar circunstancias que afectan la seguridad de una infraestructura. Además, importante es tener en cuenta que la tecnología no se detiene, aunque exista las condiciones mínimas de seguridad, estas pueden quedar fácilmente en el ayer, de ahí la importancia de seguimiento continuo.

Toda infraestructura tecnológica está compuesta por una serie de componentes de hardware y software que realizan procesos de manejo de datos, es menester que la institución mantenga un compromiso y disponga de un plan de mejora continua de actualización y fortalecimiento de estos activos, una adecuada gestión de control de riesgos genera buenos resultados de seguridad de los datos. El uso de métodos de evaluación, de dispositivos firewall físicos y lógicos de vanguardia y sistemas de auditoría sirven para salvaguarda la infraestructura y la información.

El termino seguridad[10] este siempre se entiende que busca la gestión de riesgos, entre otras palabras, prevenirlo o evitarlo y tener la oportunidad de realizar acciones preliminares para evitarlo, la seguridad podría ser llamada como la ausencia de riesgo; involucrando para su propósito las siguientes cuatro acciones, prevención del riesgo, transferir el riesgo, mitigar el riesgo, y aceptar el riesgo. Cuando hablamos de infraestructura sin duda alguna en ella se aplica efectivos controles, pero, eso no quiere decir que no tiene riesgos. Por el contrario, los riesgos vienen hacer más complejos, entre los que se dan acceso no permitido, robo de identidad y sustracción de información.

El Estado Colombiano ha hecho su pronunciamiento cuando de seguridad tecnológica se trata, elevando a rango constitucional, ley, proceso disciplinario para mantener el mínimo de las medidas de seguridad en cabeza del sector público. El

[10] ROMERO CASTRO, Martha I. otros... “Ingeniería y Tecnología. 3Ciencias. Introducción a la Seguridad Informática y el Análisis de Vulnerabilidades”, 2018. p,3.

incumplimiento de las políticas de seguridad conlleva adelantar procesos disciplinarios o legales a que haya lugar.

6.1 PROCEDIMIENTOS DE SEGURIDAD

6.1.1 Copias de Seguridad

Sin duda alguna toda institución debe contar con un plan sistemático de copias de seguridad, colocar la información a buen recaudo es sin duda una de las mejores decisiones en lo que respecta a medidas acordes para hacer frente a perdidas de información por contingencias que se pueden presentar por amenazas o error del administrador encargado.

La ejecución organizada de los Backus de la información que maneja la institución permite que sea continuo el desarrollo de las funciones, permite entonces el cumplimiento de su objeto social, siendo positivo este procedimiento para afrontar diferentes tipos de amenazas bien sea por ciberdelincuente, accidentes y errores a los cuales no se está exento, no sobra de ninguna manera la implementación de esta medida para la protección de un activo tan valioso como es la información.

Es indispensable este procedimiento determinar qué información es la que será objeto de una copia de seguridad, el inventario de los activos de información y la clasificación de criticidad para la institución bien sea tangible o física de ficheros varios, contar con el registro del procedimiento es imprescindible para la institución en el tiempo oportuno establecido en el plan definido para mantener la disponibilidad del activo bajo la supervisión del administrador.

6.1.2 Almacenamiento en la nube

La utilización de almacenamiento en la nube es una excelente opción al momento de tomas medidas para salvaguardar la información, son múltiples los servicios que se encuentran en el mercado en lo que tiene que ver esta opción de almacenamiento, establecer criterios claros acerca de lo que puede guardarse es fundamental, inclusive una buena apuesta a tener en cuenta para salvaguardar son las copias de seguridad con una exigencia clara de las garantías necesarias de seguridad por parte de servidores de terceros.

Son varios los motivos positivos para realizar almacenamiento de la información en la nube, entre otra la disponibilidad para acceder a la información desde cualquier lugar, recursos optimizados, y control de los permisos de acceso. La institución debe mantener las políticas de clasificación y control de la información que puede subirse.

6.1.3 Control de Acceso a información sensible

La implementación del control de acceso a usuarios es de vital importancia y significativo en la institución y organización, la política de control de acceso permite asegurar los datos importantes y mantener el sistema de seguridad de ingreso permitido, mejorando notablemente con eficacia la administración de la información como activo valioso, este sistema garantiza que los usuarios que ingresan al sistema son los que son y lo hacen a través de la prueba de identidad que viene siendo el método de autenticación.

Es más que necesario contar con esta política de seguridad para ayudar a la protección de la información y evitar contratiempos de ingresos no autorizados que ponen en riesgo la información y los servicios de la infraestructura, pueden tenerse en cuenta de acuerdo con la necesidad existente uno de los siguientes tipos de control de acceso existentes, basado en roles (RBCA) se ejecuta para acceder tanto a los datos como al recurso del sistema, discrecional (DAC) determina quién puede tener acceso al determinado archivo y se muestra como la autorización del propietario o administrador que puede ser cambiable cuando el caso amerite, obligatorio (MAC) el administrador determina quien puede acceder a recursos muy confidenciales podría decirse que muy secretos, y basados en atributos (ABAC) siendo un método más dinámico pero sin tanta amplitud en el acceso por cuanto se le imprimen una serie de atributos. Por tanto, la aplicación de estas medidas es esencial y realizan una tarea importante en la seguridad de la información.

6.1.4 Creación de contraseñas seguras

Siempre se ha buscado a lo largo del tiempo proteger las cosas más valiosas que están dentro del baúl con un buen candado y llave, de igual forma las organizaciones quieren mantener ese bien precioso de la información bajo la seguridad que sea necesaria sin considerarla exagerada cuando de ella se trata, de ahí la que las contraseñas deben ser seguras y robustas para evitar que se ponga en riesgo el activo valioso de la información, nace entonces la ingeniosidad de la aplicación de medidas mediante variados mecanismos para la creación de contraseñas seguras y robustas y no es para menos, debido a los avances tecnológicos esta tarea demanda la atención para no hacer tan fácil la actividad delincuencial de los atacantes cibernéticos.

Buscar que todo tipo de proceso realizado en la institución sea sin riesgo es un objetivo permanente y que no debe pasarse por alto en ningún momento, deben tenerse en cuenta todas las medidas para evitar ser sorprendido, recordar que las ataques están al acecho y que no puede bajarse la guardia porque los resultados pueden ser nefastos para el usuario como para la institución.

La contraseña es esa llave que debemos guardar con mucho cuidado, nos permite tener un acceso seguro a cualquier medio tecnológico y donde hemos tenido la

oportunidad de crear la contraseña bien sea de manera personal o por medio de un administrador, de ahí que no puede olvidarse de la importancia de la contraseña. Las contraseñas deben cambiarse periódicamente al menos cada 90 días, la utilización de contraseñas robustas donde incluya números y caracteres mayúsculas, minúsculas y símbolos, su longitud al menos de 9 caracteres, no tener caracteres consecutivos evitando que estas no sean débiles y mantengan fragmentos de nombres; una adecuada utilización de las contraseñas exige que estas no sean rebeladas a ninguna persona, evitar contraseñas similares, en licencias o vacaciones no cederlas, y como tampoco compartirlas en documentos o solicitudes electrónicas. Es importante la participación responsable y buenas prácticas del usuario en el uso de las contraseñas que aporta la seguridad de la infraestructura tecnológica y la seguridad del activo de la información.

6.1.5 Protección del correo electrónico

Contar con las medidas necesarias en todos los dispositivos de la infraestructura es sin duda una tarea ardua, igualmente el correo electrónico institucional hace parte de esos medios a los debe aplicarse las medidas de seguridad necesarias, por medio de él se mueve mucha información valiosa y confidencial que puede verse en riesgo por falta de buenas prácticas y medidas necesarias ante vulnerabilidades o amenazas que acechan permanentemente el camino que deben andar los mensajes antes de llegar a su destinatario.

Algunos de esos riesgos que están presentes, la inundación, producida por sobrecargado del sistema producido por el atacante; correo masivo (spam), conocido como el correo basura; y confidencialidad la cual debe estar protegida por la encriptación, cuando está ausente está en el correo el mensaje puede ser leído por un ciberdelincuente, ataques de ingeniería social que logra trasmitir confianza falsa sin sospechas para que no se logre identificar que se trata precisamente de un ataque.

6.1.6 Uso de software DLP

Cuando hablamos de DLP (Prevención de pérdida de datos) nos redirecciona inmediatamente a las medidas que deben tomarse dentro de la institución para contrarrestar la fuga de la información que se pueda estar presentando, esta herramienta es una excelente opción para amparar de manera preventiva la fuga de información valiosa, esta se puede presentar en algunos casos de manera no intencional, de ahí que dicho software permite capacitar a los usuarios sobre la manera adecuada del manejo de la información lo cual es bastante beneficioso.

Este software trabaja de una manera efectiva ayudando a la detección, monitoreo, protección y prevención en tiempo real la fuga de información sensible que se pueda estar presentando en la institución u organización, recordar que la perdida de información es el problema que más afecta y exige el máximo de cuidado para

evitarlo, el DLP administra la información y dependiendo de su categorización, almacenamiento y propietario identificado realiza la detección de información sensible y crea un inventario sobre esta y su dueño, supervisa la manera que se maneja la información, protección de la información empleando de manera automática las políticas de seguridad, administra política global sobre fuga de información en toda la institución u organización, identifica también incidencias de seguridad y presenta informes correspondientes.

La implementación del DLP es cuestión para especializados, tratándose de una herramienta que protege el activo valioso de la institución y sus tipos DLP de red, DLP host son ubicados en la periferia de la red como también al interior de la red (servidores, equipos y portátiles) donde se encuentra la información valiosa.

6.1.7 Monitorización y respuesta inmediata

El monitoreo de la infraestructura mediante planes organizados se presenta como la mejor manera de atender a tiempo las incidencias de seguridad que se puedan presentar, el administrador cuenta con una gran oportunidad de la detección de vulnerabilidades y amenazas que se puedan estar presentando sin necesidad a que estas sean reportadas por el usuario, siendo provechoso para los servicios que atiende la infraestructura tecnológica.

Los activos físicos que componen la infraestructura, el activo de la información, y la institución se ven favorecida de una política organizada de monitore permanente con informes detallados, es una tarea ardua que demanda de tiempo y experiencia para la obtención de resultados que deben ser analizados en detalle por el líder, la ejecución de una de las variadas herramientas acorde es fundamental y de gran ayuda para la identificación de las deficiencias de seguridad, su adquisición no debe omitirse por ningún motivo, pues de ella depende junto con la experiencia del líder de saber cuál es estado de salud de la infraestructura.

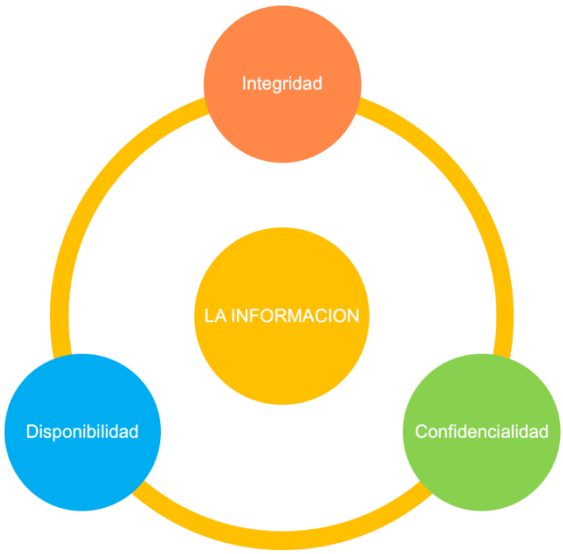
Del resultado del monitoreo a tiempo de la infraestructura además de ser preventiva, también se puede tomar las respuestas necesarias y acordes en caso de encontrarse vulnerabilidades y amenazas que ameritan decisiones de solución inmediata, para tomar el control y velar en todo sentido por el activo de la información y demás recursos con el uso de herramientas de gestión de seguridad, experiencia y mejores prácticas que traen como resultado final la optimización de la infraestructura y minimización de costos para la institución.

7 ACCIONES PARA ENDURECER LA SEGURIDAD DE LA INFORMACION

La información es uno de los insumos valiosos para cualquier gestión que desarrollan las instituciones en Colombia, implantar políticas contundentes, y definidas permiten adelantar una efectiva gestión en el almacenamiento, administración y transmisión. Los lineamientos de seguridad encaminados a minimizar la alteración, sustracción, fuga o disponibilidad. De acuerdo con este contexto de políticas para la protección de la información aplica acciones robustas para la definición de lineamientos, controles, responsabilidades para la tarea de manejo de la información; Control y gestión de amenazas de los sistemas de información; y limitar la capacidad de los delincuentes informáticos.

Es preciso indicar que todas instituciones de educación media en Colombia deben tomar atenta nota para aplicar políticas solidas de protección de manera continua sin escatimar recursos para mantener apropiadamente la confidencialidad, integridad y disponibilidad del activo valioso.

Figura 2. Pilares de la información.



Fuente: Propia

Integridad: La información mantiene su originalidad ante cualquier ataque o intento de sustracción, solo podrá ser modificada por autorización. Confidencialidad: Que se presenta las medidas de protección adecuadas para evitar su divulgación sin consentimiento, solamente sea accesible a personas autorizadas. Disponibilidad: La información no debe tener inconveniente alguno para su consulta o acceso en cualquier momento para la respectiva productividad educativa de la institución.

Para el desarrollo de acciones de endurecimiento de la seguridad de la información debe estar acompañada de las medidas de configuración de los dispositivos que conforman la infraestructura tecnológica, la cual juega papel importante para la obtención de la protección de la información; entre ellos firewall, sistemas de detección de intrusos, y sistemas de identificación y administración de amenazas.
La norma ISO/IEC 27001[11], establece una serie de medidas y recomendaciones esenciales que no deben pasarse por alto en una institución para asegurar la protección de la información. Esta norma contempla 10 dominios: 1. Política de Seguridad de la Información, 2. Organización de la Seguridad de la Información, 3. Gestión de Activos, 4. Seguridad de Recursos Humanos, 5. Seguridad Física y del Entorno, 6. Gestión de Comunicaciones y Operaciones, 7. Control de Acceso, 8. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información, 9. Gestión de Incidentes de la Seguridad de la Información y, 10. Cumplimiento

Además, es de suma importancia el factor humano que según Laudon[12], K. C. y Laudon, J. P. (2012) y Saroka, R. H. (2002), "muchas de las debilidades de los sistemas provienen del factor humano más que de aspectos técnicos. Además, si bien gran parte de las amenazas vienen del exterior de la empresa, la mayoría surgen desde el interior de esta donde los empleados pueden representar un problema en la seguridad. Los trabajadores tienen un acceso privilegiado a la información y a los sistemas, pudiendo robar, modificar o borrar los datos sin dejar rastros cuando la seguridad no es la adecuada".

7.1 EL ENDURECIMIENTO

La implementación de endurecimiento con seguridad perimetral indicada para la infraestructura de una Institución educativa de educación media de la ciudad Ibagué, incluye las distintas políticas de seguridad actuales y de avanzada plena atención y aplicación de los modelos internacionales de buenas prácticas tecnológicas, permitirá a la institución de educación minimizar riesgos, control de vulnerabilidades, prevención de amenazas de los activos, y toma de decisiones acertadas ante cualquier incidencia de seguridad.

Los dispositivos que se especifican adelante con los que contará las infraestructura son los adecuados para solucionar la necesidad de la institución, cuentan con tecnología de nueva generación y con las debidas configuraciones de harán frente a las diferentes amenazas que han evolucionado y que hoy se presentan como avanzadas, con respaldo de experiencia de varios fabricantes expertos en seguridad de infraestructuras, acompañados de personas especializadas y con

[11] VELASCO MELO, Arean H. "Revista de Derecho. El Derecho Informático y La gestión de la Seguridad de la Información Una Perspectiva con Base en la Norma ISO 27001", 2008
[12] Laudon , K. C. otros… "Trabajo de Investigación, Seguridad Informática: La Protección de la Información en Una Empresa Vitivinícola de Mendoza". 2019. p, 40.

experiencia en infraestructuras formarán la mejor estrategia defensa para mantener protegidos sus procesos, sin desmejora del rendimiento de red, reduciendo los riesgos, incrementando el uso de la información, y fijando las bases para la tecnología del futuro.

7.2 EXPERTOS EN EL PROCESO DE ENDURECIMIENTO

Participaran para el fortalecimiento de la infraestructura ingenieros de sistemas especializados de acuerdo con su conocimiento y experiencia en la implantación de activos físicos y lógicos para asegurar su funcionalidad y efectividad en los procesos de seguridad para beneficio de la organización, comprometidos los siguientes:

7.2.1 Líder del proyecto infraestructura,

Su rol de desarrollar el proyecto de endurecimiento de la infraestructura, con amplio conocimiento y experiencia en procesos de seguridad, encargado de los proveedores, participa directamente en las actividades de implantación de los dispositivos, orienta la ejecución del plan de actividades por los demás expertos y realiza las revisiones necesarias, responsable de la terminación y entrega del proyecto al líder de la Infraestructura designado por la Institución.

7.2.2 Analista de sistemas

Se encarga en este proyecto del diseño del sistema, análisis de general y especifico, diseño e implementación de la base de datos y adecuación de esta, y de las configuraciones de operación y funcionalidad con seguridad.

7.2.3 Diseñador

Su función estará basada en la implementación de un sistema que satisfaga la necesidad de la institución y que este permita cumplir su objetivo, que cumpla con las especificaciones de acceso, uso, interactividad, y garantizando que este se interconectará con las tareas a realizar por el usuario.

7.2.4 Responsable de Configuración y Pruebas

Su responsabilidad en este proyecto es de amplia actividad centrada en los componentes, asegurando la funcionalidad correcta de cada dispositivo, haciendo las pruebas que considere necesarias para lograr el ajuste adecuado de todo el software y que este trabaje con plena correspondencia con el activo físico implantado, además de la plena disponibilidad y funcionalidad.

El trabajo de los profesionales se ajustará plenamente al trabajo en equipo con el propósito de lograr la integración de conocimiento para la efectivización de las actividades del proyecto en pro del adecuado endurecimiento de la infraestructura.

7.3 ENDURECIMIENTO DE SOFTWARE

7.3.1 IDS/IPS Y FUNCIONAMIENTO

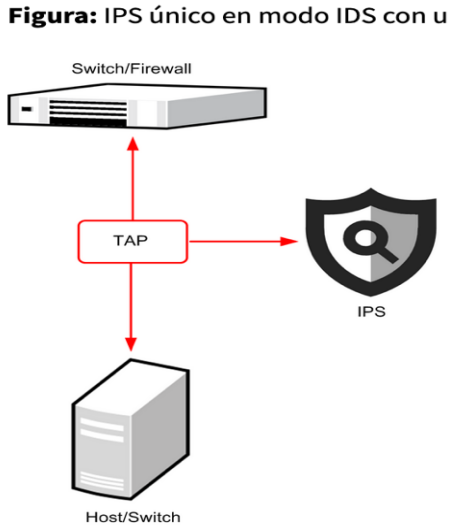
Se encarga de la tarea de monitorear en tiempo real el tráfico de la red entrante para la detección de intrusos, teniendo la capacidad de reconocer cuando se trata de un ataque de intrusión no permitida a la infraestructura inmediatamente realiza la evaluación teniendo la base de datos de ataques de firmas de ataques, procediendo a descartar paquetes y de ser necesario la desconexión.

IDS, su actividad principal la de detectar accesos no autorizados mediante el monitoreo del tráfico entrante de la red, hace comparativa con las firmas de ataques actuales, alguna siendo positiva, genera una alerta al líder de la red para que tome las medidas necesarias.

IPS, analiza mediante escaneo en tiempo real de conexiones y protocolos para la detección de ataques e intrusos, actúa de manera preventiva, de acuerdo con patrones tiene la capacidad de identificar una actividad sospechosa, generando una alerta al administrador de la red, e inmediatamente ejecuta el bloqueo de la conexión o la de descarte.

Se colocará IDS/IPS Forcepoint para la prevención de intrusos, teniendo en cuenta que las especificaciones y características del modelo series 1100 ofrecen la seguridad requerida, trabajando:

Figura 3. IDS-IPS series 1100 Forcepoint



Fuente: Forcepoint NFFW. Implementación IPS en modo IDS. [En línea]. [Recuperado 16 noviembre 2022). Disponible en: https://help.stonesoft.com/onlinehelp/StoneGate/SMC/6.8.0/GUID-23A79CAC-CCC6-4C74-BE2C-85FEC9BC3D92.html

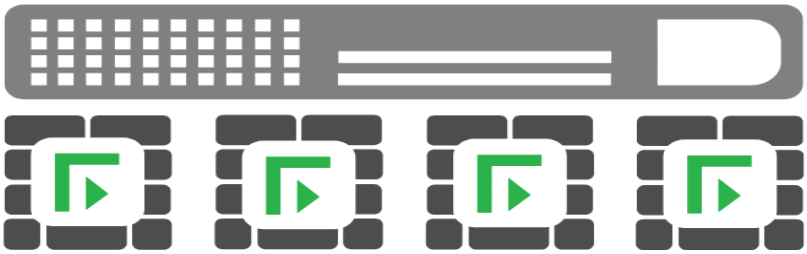
7.3.2 Firewall Virtualizado

Solución de seguridad NGFW muy diversa, su ventaja de trabajo en entornos de nube pública y privada cumple de manera efectiva las funciones de un firewall tangible, con tecnología avanzada fundamental para la infraestructura de la institución, en esencia es un software para el análisis, gestión, control y prevención de amenazas.

Su actividad de seguridad la ejecuta con métodos de filtrado del tráfico de entrada y salida de la red, filtrado de contenido, denegación de servicios DDoS, brinda políticas de seguridad dirigidas en las aplicaciones, protección en el tráfico de la nube, seguridad en el DNS, prevención de intrusión, en los entornos virtuales reduce ataques, y protección contra programa maligno siendo de vital importancia su implementación por cuando reduce costos para la institución.

Se implantará en el fortalecimiento el modelo series 1100 Forcepoint, licencia y especificaciones que se ajustan al nivel de seguridad requerido.

Figura 4. Firewall virtualizado Forcepoint.



Fuente: Forcepoint. Firewall NGFW series 1100 2022. [En línea]. [Consultado 16 noviembre 2022). Disponible en: https://www.forcepoint.com

7.4 ENDURECIMIENTO DE HARDWARE

7.4.1 Firewall físico

La implementación de un firewall físico de (NGFW), no sobra cuando se trata de seguridad de la información y de la infraestructura de la Institución u organización, una excelente opción con una mayor estabilidad, ausencia de manipulación fácil, gestión de tareas de permitir o denegar servicios y bloqueo de aplicaciones sospechosas.

El firewall Forcepoint posee tecnología perimetral de nueva generación, proporciona un nivel de seguridad adecuado con las exigencias de la institución educativa de

educación media, con funcionalidad de prevención de ataques y seguridad en los servicios de información de la infraestructura.

Su modelo NGFW 1100 permite cubrimiento de rendimiento y protección de amenazas externas y junto con el firewall virtualizado para la protección interna de dispositivos específicos, presentándose como opción oportuna para el espacio donde se implementará, con especificaciones que se muestran en las siguientes graficas:

Figura 5. Firewall NGFW Forcepoint

Fuente : Forcepoint. Firewall Forcepoint séries 1100. [En Línea]. NGFW 2022. [Recuperado 16 noviembre 2022]. Disponible en: https://www.forcepoint.com

Cuadro 1. Especificaciones Firewall NGFW series 1100.

PERFORMANCE[1]	N1101	N1105
NGFW/NGIPS throughput (HTTP 21kB payload)	1.5 Gbps	3 Gbps
Max firewall throughput (UDP 1518 byte)	50 Gbps	60 Gbps
Max inspection throughput (UDP 1518 byte)	3 Gbps	6 Gbps
TLS 1.2 inspection performance (44kB payload)	800 Mbps	1.6 Gbps
IPsec VPN throughput AES-GCM-256	4.5 Gbps	8.5 Gbps
Concurrent IPsec VPN tunnels	20,000	
Mobile VPN clients	Unlimited	
Concurrent inspected TCP connections	500,000	1 million
Max number of concurrent inspected HTTP connections	450,000	1 million
VLAN tagging	Unlimited	
Virtual contexts default/maximum	5/25	10/100

Fuente: Fuente: Forcepoint. Firewall Forcepoint series 1100. [En línea]. NGFW 2022. [Recuperado 16 noviembre 2022]. Disponible en: https://www.forcepoint.com

Cuadro 2. Características Firewall NGFW series 1100

PHYSICAL	N1101	N1105
Form factor	1RU	
Dimensions W x H x D	439 x 44 x 300 mm 17.28 x 1.73 x 11.81 in	
Net weight without modules	4.8 kg 10.58 lbs	
AC power supply	100 - 240 VAC 50 - 60 Hz, 180 W	
Typical power consumption	60 W	70 W
Max power consumption	95 W	100 W
Max BTU/hour	324	341
MTBF	100,000 hours	
Operating temperature	0° - 40° C, 32° - 104° F	
Storage temperature	-20° - 70° C, -4° - 158° F	
Relative humidity non-condensing	10% - 95%	
Safety certifications	CB, UL/EN60950, BSMI, CTICK, NOM	
EMI certifications	FCC Part 15, CE, EN55022, EN55024, VCCI-CISPR	

Fuente: Fuente: Forcepoint. Firewall Forcepoint series 1100. [En línea]. NGFW 2022. [Recuperado 16 noviembre 2022]. Disponible en: https://www.forcepoint.com

7.4.2 Router

Este dispositivo también se conoce como “enrutador o encaminador” de paquetes, trabaja proporcionado conectividad a nivel de red, su funcionalidad la desarrolla al enviar paquetes de datos de una red a otra, entre otras palabras, interconectar subredes o varias máquinas que se pueden comunicar entre sí por medio de IP. Su participación de seguridad en la infraestructura viene siendo como la de un policía de tráfico, porque todo el tráfico interno va a través de él, dirigen el tráfico, es el filtro o defensa inicial y final.

Se decide por el uso de este Router TWG-431BR por contar con especificaciones acordes a lo que requiere implantar y sus características se describen en las siguientes figuras:

Figura 6. Router Gigabit multi-WAN VPN TWG-431BR (Versión v1.0R)

Fuente: Trendnet. Router empresarial. [En línea]. [Recuperado 15 de noviembre de 2022]. Disponible en: https://www.trendnet.com/langsp/products/business-router/gigabit-multi-wan-vpn-business-router-TWG-431BR

Cuadro 3. Especificaciones Router Gigabit multi-WAN VPN TWG-431BR

DESCRIPCIÓN	ESPECIFICACIONES	DESCARGAS / SOPORTE TÉCNICO	VER EMULADOR
Normas	• IEEE 802.3 • IEEE 802.3u • IEEE 802.3x • IEEE 802.3ab • IEEE 802.1Q		
Interfaz del dispositivo	• 5 puertos Gigabit (modos: 4 puertos WAN / 1 puerto LAN o 1 puerto WAN / 4 puertos LAN) • 1 puerto USB 3.0 (configuración de copia de respaldo y restauración / Exportación de registro) • 1 puerto de consola RJ-45 • Botón de reinicio • Indicadores LED		
Funcionamiento	• Transmisión NAT (LAN a WAN): 900Mbps • Rendimiento de enrutamiento: 900Mbps • Máximo de sesiones concurrentes: 50,000 • Número máximo de VLAN: 8 (ID: 1-4093) • Transmisión IPsec VPN (AES-256/SHA-256/LAN a LAN): 200Mbps • Transmisión SSL VPN (Blowfish/SHA-1/puente): 20Mbps		
VPN	• SSL VPN de Cliente a Sitio (hasta 30 túneles) • IPsec VPN de Sitio a Sitio / de Cliente a Sitio (hasta 40 túneles) • Servidor PPTP/L2TP VPN / de Cliente a Sitio (hasta 40 túneles) • L2TP con Servidor IPsec VPN / Cliente a Sitio (Hasta 40 túneles compartidos con L2TP) • Encriptación IPsec: 3DES, AES-128/192/256 • Autenticación IPsec: MD5, SHA-1, SHA-256 • Intercambio de clave IPsec: IKE: Modo principal/agresivo, clave precompartida, grupos DH 1/2/5/14 • Protocolos IPsec: ESP, PFS DH grupos 1/2/5/14, DPD, ID local/remota: Dirección IP, FQDN • IPsec NAT Traversal • Encriptación SSL VPN: AES • Certificado SSL VPN: RSA • Encriptación PPTP/L2TP: MPPE 40 bits, 128 bits, IPsec • Autenticación PPTP/L2TP MS-CHAPv1/2		
Trabajo en red	• Modos WPS: NAT, enrutamiento clásico • Modos NAT: NAT, PAT • Modos IPv4 WAN: DHCP, IP estática, PPPoE, PPTP • Modos IPv6 WAN: Estático, Autoconfiguración (SLAAC/DHCPv6), Link-Local, PPPoE, 6to4, 6rd • Enrutamiento: Estático, dinámico RIPv2, OSPFv1/2, distribución de RIPv2 por OSPFv1/2, políticas de enrutamiento (hasta 20 entradas) • Enrutamiento inter-VLAN (hasta 8 VLAN, 8 interfaces IP) • Servidor DHCP/relé • DNS dinámica: dyn.com, no-ip.com • WAN Failover • Balance de cargas WAN: Asignación de pesos por porcentaje o ancho de banda, basada en IP de origen, basada en IP de origen y destino, basada en sesión • Alta disponibilidad: Admite un 1 clúster activo-pasivo hasta un total de 6 unidades (1 maestra + 5 en espera) • VPN passthrough: IPsec, PPTP, L2TP		

Fuente: Trendnet. Router empresarial. [En línea]. [Recuperado 15 de noviembre 2022]. Disponible en: https://www.trendnet.com/langsp/products/business-router/gigabit-multi-wan-vpn-business-router-TWG-431BR

7.4.3 Switch.

Es un medio de interconexión, trabaja en la capa 2 (MAC), Inspeccionando la dirección origen y destino del paquete para establecer la ruta de intercambio. Permitiendo interconectar múltiples dispositivos a la red, muy usado en instituciones u organizaciones.

Se implantará en el endurecimiento de la infraestructura de la Institución el Switch ZyXEL, el cual de acuerdo con las especificaciones técnicas cumple con las exigencias necesarias del servicio. En los siguientes gráficos se muestran las características:

Figura 7, ZyXEL GS1900-24 L2 24p Gigabit - Switch

Fuente: Coolmod. ZyXEL-Switch [En línea]. Artesanos del Gaming. [Consultado 14 noviembre 2022]. Disponible en: https://www.coolmod.com/zyxel-gs1900-24-l2-24p-gigabit-switch/

Cuadro 4. Detalles modelo ZyXEL GS1900-24 L2 24p Gigabit - Switch

Marca	ZyXEL
Modelo	**GS1900-24-EU0101F**
Puertos	- 24 puertos GbE de Smart Switch gestionable con GbE de enlace ascendente
	Stándares
	- IEEE 802.3 10BASE-T Ethernet
	- IEEE 802.3u 100BASE-TX Ethernet
	- IEEE 802.3ab (1000BASE-T) Ethernet
	- IEEE 802.3x flow control
	- IEEE 802.3az EEE support
	- IEEE 802.1p CoS support
	- IEEE 802.1D Spanning Tree Protocol (STP)
	- IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)
	- IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)
	- Full-duplex and half duplex operation with IEEE 802.3x flow control and backpressure
	- Store and forward
	- Auto MDI/MID-X

Fuente: Coolmod. ZyXEL-Switch [En línea]. Artesanos del Gaming. [Consultado 14 noviembre 2022]. Disponible en: https://www.coolmod.com/zyxel-gs1900-24-l2-24p-gigabit-switch/

Cuadro 5. Características de ZyXEL GS1900-24

Características	- BPDU guard - Static MAC forwarding - RADIUS - TACACS+ - SSL - Management VLAN - CPU defense engine - DoS prevention **Layer 2 Multicast** - IGMP snooping (v1,v2,v3) **IPv6** - IPv6 over Ethernet (RFC 2464) - Dual-stack (RFC 4213) - ICMPv6 (RFC 4884) - Neighbor discovery (RFC 4861) - Auto configuration - Static IPv6 address and prefix length - Static IPv6 default gateway - IPv6 duplicate address detection **Descubrimiento** - IEEE 802.1 AB LLDP - LLDP-MED **Gestión de red** - SNMP v1,v2,v3 - RMON (1,2,3,9) - ICMP echo/echo reply - Syslog **MIB** - RFC 1213 MIB II - RFC 2819 RMON (group 1,2,3,9) - RFC 1215 generic traps - RFC 1493 bridge - Private MIB **Certificaciones** - EMC: CE, FCC, C-Tick, Class A, BSMI CNS13438 - Safety: LVD EN60950-1, BSMI CNS14336-1, CB IEC60950-1 - RoHS compliant **Alimentación** - Voltaje de entrada AC: 100 - 240 V AC, 50/60Hz- Consumo: 16 W **Físicas** - Dimensiones(An x Prof x Al): 440 x 131 x 44

Fuente: Coolmod. ZyXEL-Switch [En línea]. Artesanos del Gaming. [Consultado 14 noviembre 2022]. Disponible en: https://www.coolmod.com/zyxel-gs1900-24-l2-24p-gigabit-switch/

7.4.4 Servidores

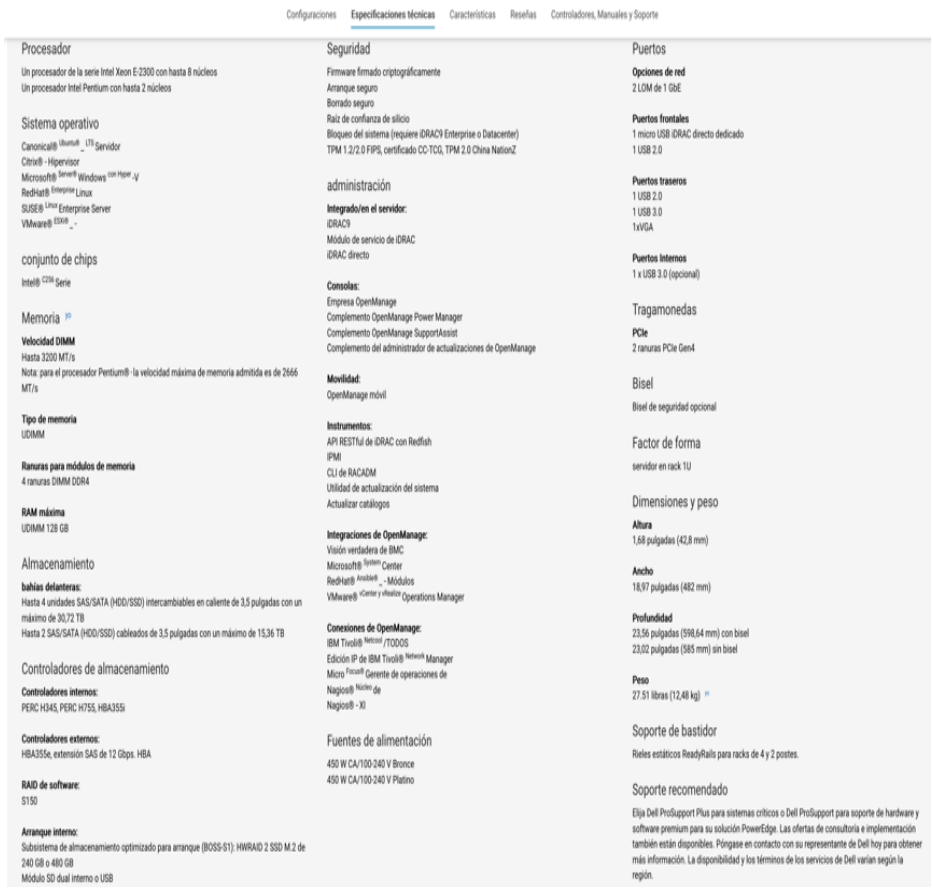
Son dispositivos que suelen prestar servicios esenciales y dedicados a responder los requerimientos de un cliente, como su nombre lo describe es una máquina que está al servicio de otras. Estos trabajan en distintos campos dependiendo el que le sea asignado por el líder de la infraestructura.

Se instalará los servidores exigidos en la infraestructura de solución de la institución el PowerEdge R250 de la compañía Dell que se ajusta a las exigencias según las especificaciones descritas en las siguientes imágenes:

Figura 8. Servidor en rack PowerEdge R250

Fuente: Dell. Servidores en rack PowerEdge. [En línea]. Soluciones y servicios Dell. [Consultado 19 noviembre 2022]. Disponible en: https://www.dell.com

Cuadro 6. Especificaciones técnicas



Configuraciones | Especificaciones técnicas | Características | Reseñas | Controladores, Manuales y Soporte

Procesador

Un procesador de la serie Intel Xeon E-2300 con hasta 8 núcleos
Un procesador Intel Pentium con hasta 2 núcleos

Sistema operativo

Canonical® Ubuntu® LTS Servidor
Citrix® - Hipervisor
Microsoft® Server® Windows con Hyper-V
RedHat® Enterprise Linux
SUSE® Linux Enterprise Server
VMware® ESXi® -

conjunto de chips

Intel® C256 Serie

Memoria

Velocidad DIMM
Hasta 3200 MT/s
Nota: para el procesador Pentium® - la velocidad máxima de memoria admitida es de 2666 MT/s

Tipo de memoria
UDIMM

Ranuras para módulos de memoria
4 ranuras DIMM DDR4

RAM máxima
UDIMM 128 GB

Almacenamiento

bahías delanteras:
Hasta 4 unidades SAS/SATA (HDD/SSD) intercambiables en caliente de 3,5 pulgadas con un máximo de 30,72 TB
Hasta 2 SAS/SATA (HDD/SSD) cableados de 3,5 pulgadas con un máximo de 15,36 TB

Controladores de almacenamiento

Controladores internos:
PERC H345, PERC H755, HBA355i

Controladores externos:
HBA355e, extensión SAS de 12 Gbps. HBA

RAID de software:
S150

Arranque interno:
Subsistema de almacenamiento optimizado para arranque (BOSS-S1): HWRAID 2 SSD M.2 de 240 GB o 480 GB
Módulo SD dual interno o USB

Seguridad

Firmware firmado criptográficamente
Arranque seguro
Borrado seguro
Raíz de confianza de silicio
Bloqueo del sistema (requiere iDRAC9 Enterprise o Datacenter)
TPM 1.2/2.0 FIPS, certificado CC-TCG, TPM 2.0 China NationZ

administración

Integrado/en el servidor:
iDRAC9
Módulo de servicio de iDRAC
iDRAC directo

Consolas:
Empresa OpenManage
Complemento OpenManage Power Manager
Complemento OpenManage SupportAssist
Complemento del administrador de actualizaciones de OpenManage

Movilidad:
OpenManage móvil

Instrumentos:
API RESTful de iDRAC con Redfish
IPMI
CLI de RACADM
Utilidad de actualización del sistema
Actualizar catálogos

Integraciones de OpenManage:
Visión verdadera de BMC
Microsoft® System Center
RedHat® Ansible® - Módulos
VMware® vCenter y vRealize Operations Manager

Conexiones de OpenManage:
IBM Tivoli® Netcool /TODOS
Edición IP de IBM Tivoli® Network Manager
Micro Focus® Gerente de operaciones de
Nagios® Núcleo de
Nagios® - XI

Fuentes de alimentación

450 W CA/100-240 V Bronce
450 W CA/100-240 V Platino

Puertos

Opciones de red
2 LOM de 1 GbE

Puertos frontales
1 micro USB iDRAC directo dedicado
1 USB 2.0

Puertos traseros
1 USB 2.0
1 USB 3.0
1 x VGA

Puertos Internos
1 x USB 3.0 (opcional)

Tragamonedas

PCIe
2 ranuras PCIe Gen4

Bisel

Bisel de seguridad opcional

Factor de forma

servidor en rack 1U

Dimensiones y peso

Altura
1,68 pulgadas (42,8 mm)

Ancho
18,97 pulgadas (482 mm)

Profundidad
23,56 pulgadas (598,64 mm) con bisel
23,02 pulgadas (585 mm) sin bisel

Peso
27.51 libras (12,48 kg)

Soporte de bastidor

Rieles estáticos ReadyRails para racks de 4 y 2 postes.

Soporte recomendado

Elija Dell ProSupport Plus para sistemas críticos o Dell ProSupport para soporte de hardware y software premium para su solución PowerEdge. Las ofertas de consultoría e implementación también están disponibles. Póngase en contacto con su representante de Dell hoy para obtener más información. La disponibilidad y los términos de los servicios de Dell varían según la región.

Fuente: Dell. Servidores en rack PowerEdge. [En línea]. Soluciones y servicios Dell. [Consultado 19 noviembre 2022]. Disponible en: https://www.dell.com

7.5 ENDURECIMIENTO DE CONFIGURACIÓN

7.5.1 Implementación DMZ

La Zona Desmilitarizada (DMZ) para los servidores web y correo electrónico se presenta como una medida de configuración acertada para los recursos de las institución que deben ser accesibles de la red global, la DMZ admite conexiones de internet como de la red loca de la institución de educación media, y las conexiones que se presentan desde la DMZ serán bloqueadas, reduciendo de tal manera el riesgo de ser objeto de ataques de ciberdelincuentes que puedan ocasionar daños que comprometan enormemente la infraestructura de la institución de educación.

8 DISEÑO TOPOLOGÍA DE RED CON MECANISMOS DE ENDURECIMIENTO

Teniendo en cuenta, la necesidad de la Institución educativa de educación media de la ciudad de Ibagué, de una infraestructura con medidas de seguridad eficientes y de tecnología actual, es importante y necesario presentar un diseño de diagrama de una infraestructura que reúna los diferentes mecanismos de endurecimiento los cuales son de vital importancia para la gestión de los servicios, conexiones seguras, y gestión de vulnerabilidades para evitar ataques de ciberdelincuentes que pongan en riesgo no solo la infraestructura sino también la información y sus procesos actuales.

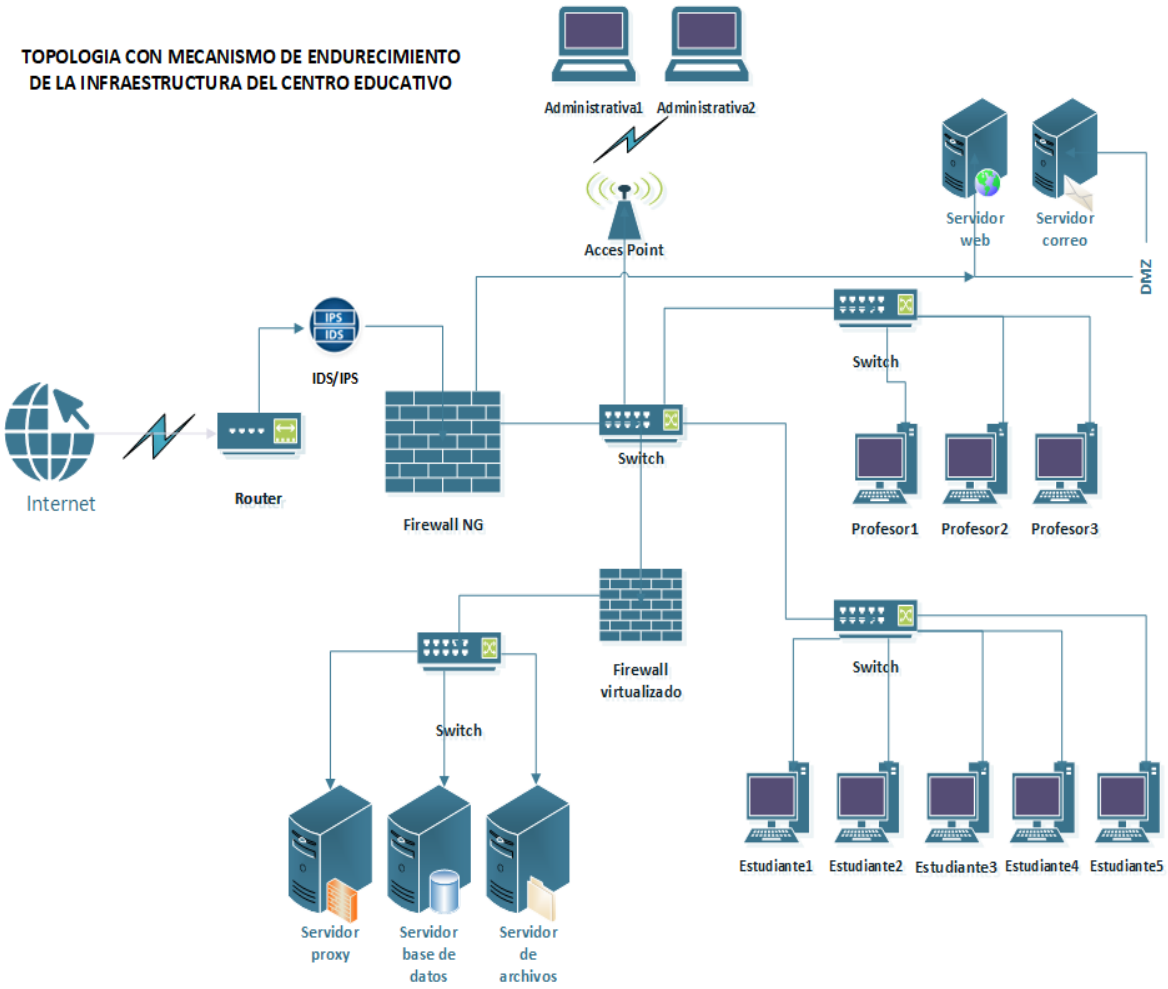
Tabla 1. Infraestructura del Centro Educativo

INFRAESTRUCTURA CENTRO EDUCATIVO

Dispositivos	Infraestructura Actual	Infraestructura con Mecanismos de Endurecimiento
Switch	Uno	Cinco. Tecnología actual
Firewall	Uno	Dos. nueva generación (NGFW), y virtualizado
Zona Desmilitarizada (DMZ)	No	Si. seguridad de los servicios web y correo, evita brecha de seguridad red interna.
Servidores	Uno	Cinco.Tecnología actual
Acces Point	No	Uno. Tecnología actual
IDS/IPS	No	Si. detección accesos no autorizados.
Router	Si	Si. Tecnología actual
Seguridad	Vulnerable	Perimetral

Fuente: Propia

Figura 9. Topología con mecanismo de endurecimiento de la Infraestructura.



Fuente: Propia

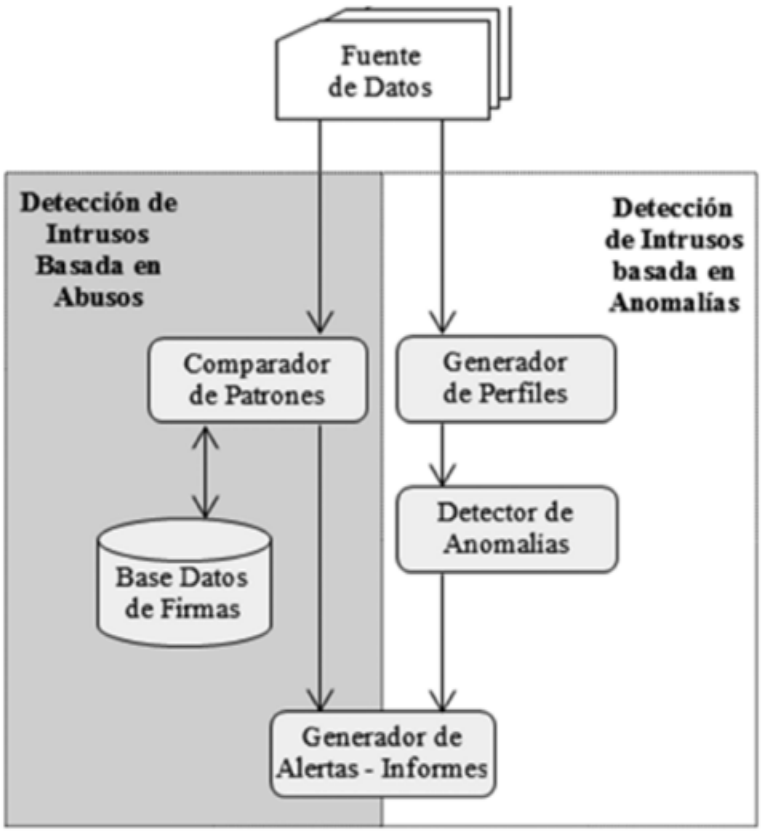
La infraestructura de la institución de educación media es fundamental y requiere precisamente de la implantación de la seguridad perimetral, armar una coraza de protección de todos los dispositivos físicos y lógicos de ser atacados por ciberdelincuentes para desestabilizar los servicios de la infraestructura y lograr la sustracción del activo de la información.

Es importante indicar la apuesta que se hace en los equipos que componen el endurecimiento de la seguridad de la infraestructura los cuales son de tecnología avanzada con el propósito de hacer una tarea efectiva acompañada de manos expertas en seguridad y de buenas prácticas incluyendo los usuarios de la institución.

8.1 LA ARQUITECTURA DE LOS DISPOSITIVOS A IMPLANTAR

Definida por las funciones que realizan y que son de esenciales en la seguridad de la red, sin desestimar que aunque la infraestructura presente una protección perimetral de última generación no quiere decir por tal que esta sea totalmente segura y que puede bajarse la guardia, por el contrario, hay que seguir con la tarea ardua de la prevención, buenas prácticas y sensibilización de los usuarios finales, porque la mayoría de ataques se presentan precisamente por los errores humanos, pero bueno sin atemorizar y afligir tanto, los beneficios que ofrece una red con seguridad de vanguardia son muchos y hay que implementarlos por necesidad para no ser una blanco permanente de los atacantes informáticos, para proteger los activos de la institución, y para realizar todos los procesos de manejo de la información de manera segura, acompañada claro con la asesoría del equipo experto en salvaguarda de la infraestructura. Se presenta el fortalecimiento de acuerdo con la necesidad de la institución de la siguiente manera:

Figura 10. Arquitectura de los IDS/IPS

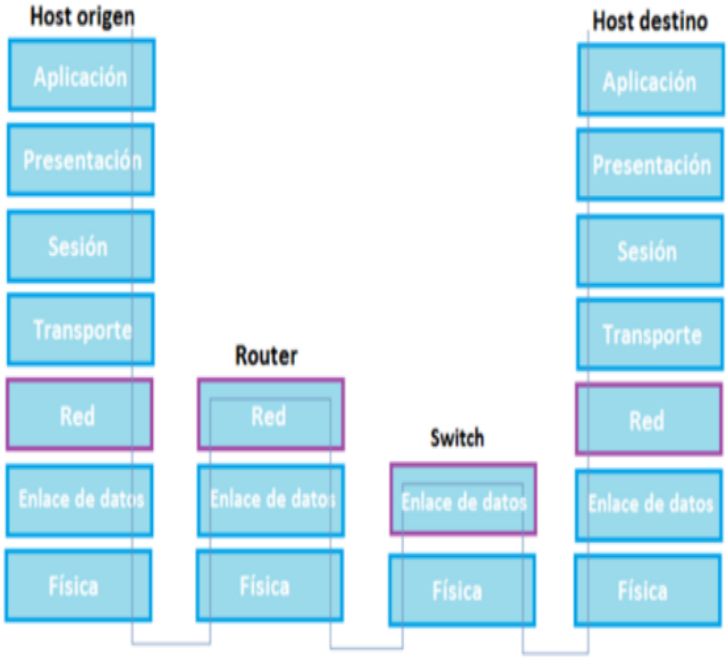


Fuente: DE LA HOZ, Emiro, otros… "Revista INGE CUC, volumen 8, numero 1, octubre de 2012," [En línea]. Detección de Intrusos. [Recuperado en 15 noviembre 2022]. Disponible en: https://revistascientificas.cuc.edu.co

Los IDS/IPS comportan dos propósitos que son la “prevención y la reacción”, en su orden la inicial es de “escucha” del tráfico en la infraestructura, con la intencionalidad de poder obtener la identificación del ataque, mediante patrones ejecuta técnicas de reconocimiento o basadas en modelos estadísticos.

En esta figura se observa la arquitectura funcional, relacionada con los algoritmos usados estratégicamente para el análisis, teniendo em cuenta los enfoques de “detección de intrusos basada en abusos y detección de intrusos basada en anomalías”.

Figura 11. Arquitectura de los Router y Switch en el modelo OSI

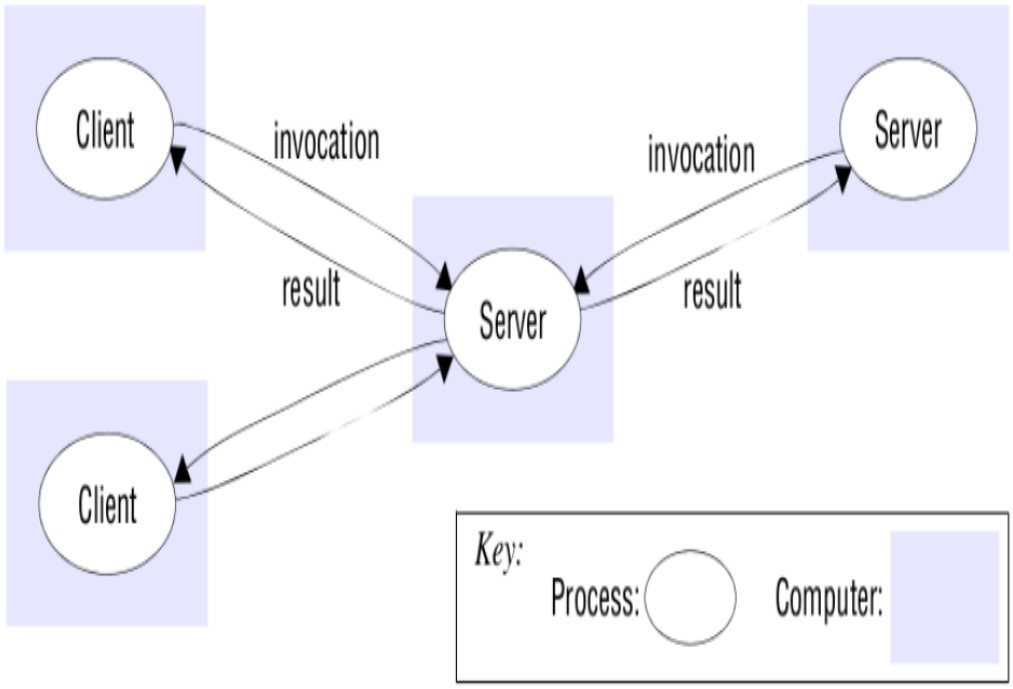


Fuente: Acomee. Router. [En línea]. Los encaminadores en el modelo OSI. [Recuperado en 17 noviembre 2022]. Disponible en: https://www.acomee.com.mx

Se distinguen en el modelo OSI, diferentes niveles que son utilizados para la comunicación entre sí se encuentran en el caso de los enrutadores dos clases de interfaces: Interfaces encaminadas, pertenecen al nivel tres con accesibilidad por IP, correspondiéndose cada una con dirección subred diferente. Se identifican en dos subtipos: Interfaces físicas, acceso directo por IP. Interfaces Virtuales, se corresponden con una LAN o CV.

Y las Interfaces conmutadas, son de nivel dos, acceso por módulo de conmutamiento, existen dos tipos: Puertos de acceso, soporta solamente tráfico de VLAN. Y Puertos trunk, soportando tráficos de varias VLANs distintas.

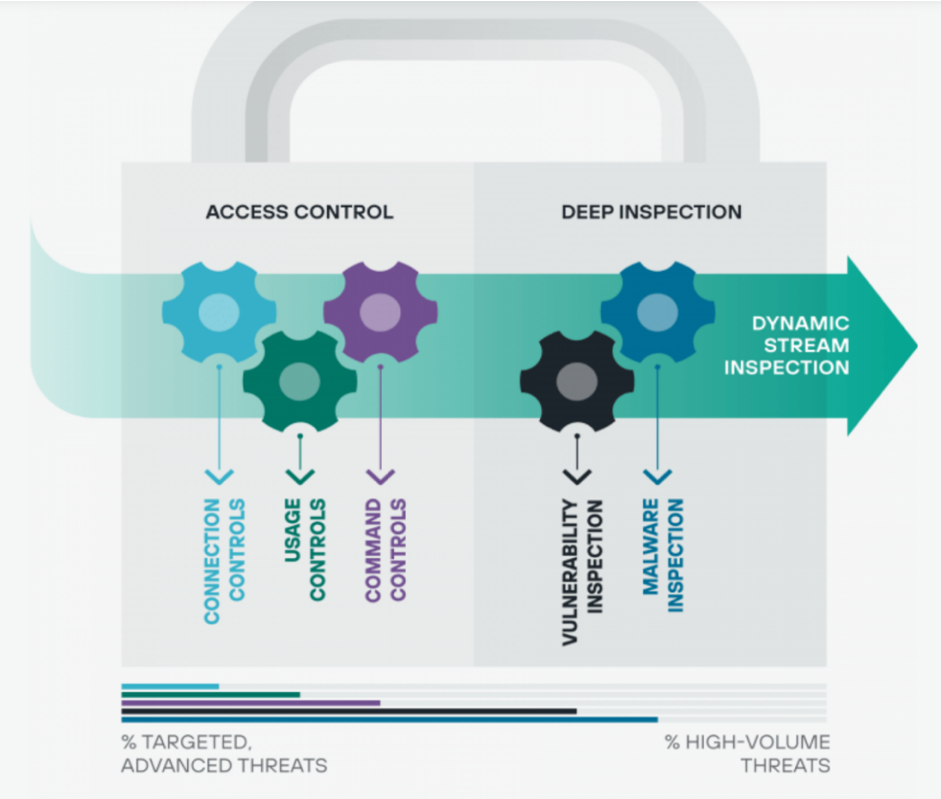
Figura 12. Arquitectura cliente - servidor



Fuente: DEYMONNAZ, Pablo, A. otro… UBAfiuba Cliente-Servidor. [En línea]. Facultade Ingeniería Universidad de Buenos Aires. [Recuperado en 16 noviembre 2022]. Disponible en: https://www.fi.uba.ar

La arquitectura de un servidor, en su concepto trata de la relación entre el usuario y un servidor cualquiera que sea su tipo en este caso servidor proxy, de base de datos, de archivos, web, y de correo electrónico, cumpliendo con una función inteligente y su competencia de procesamiento. Se presenta una gran opción de configuración desde una pequeña red hasta una red de gran capacidad de procesos. Actualmente las herramientas de un servidor vienen preinstaladas y al momento de su configuración es importante tener en cuenta las necesidades y criticidad.

Figura 13. Arquitectura Firewall NGFW Forcepoint



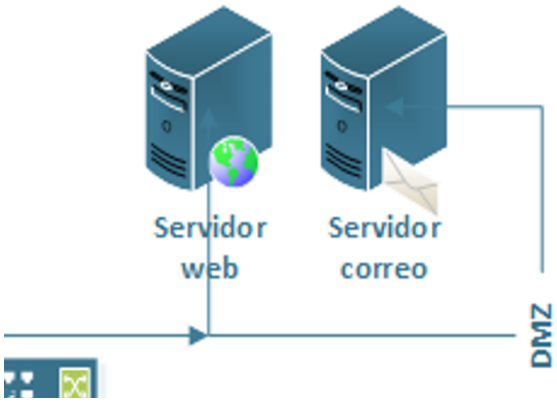
Fuente: Forcepoint. Next -Gen Firewalls. [En línea]. Logre más con menos con el Next-Gen Firewall (NGFW) de Forcepoint. [Consultado 18 noviembre 2022]. Disponible en: https://www.forcepoint.com/es/product/ngfw-next-generation-firewall

Los firewalls nueva generación inspecciona paquetes en profundidad, ofrece funcionalidades del firewall tradicional, utiliza filtrado de paquetes estático y dinámico, cuenta con soporte VPN para para que las conexiones sean seguras, tiene grandes capacidades para la filtración de paquetes de acuerdo con las aplicaciones, control extenso para identificación de aplicaciones mediante análisis y emparejamiento de firmas.

El uso del firewall físico y lógico permite una cobertura y configuración flexible para cumplir con la seguridad efectiva requerida por la infraestructura de la institución de educación media, precisamente eso es importante porque no solo habrá un control general sino también especifico permitiendo un profundo y detallado análisis que beneficia positiva las conexiones internas y externas.

El trabajo que ejerce el firewall NGFW es de alto rendimiento en la defensa de la infraestructura, su configuración es dinámica y sus controles de seguridad se despliegan rápidamente y con mayor precisión para identificar y resolver incidencias.

Figura 14. Arquitectura DZM



Fuente: Propia

Esta arquitectura de firewall con zona DMZ, es un estándar moderno con una interfaz de red adicional en el firewall, la comunicación puede presentarse de acuerdo con la configuración detallada de acceso dentro del contrafuegos. El principal objetivo de esta estructura es brindar el más alto nivel de seguridad al momento de poner a disposición servicios en internet.

En este caso se propone el cubrimiento de la zona de los servidores web y correo electrónico, lo cual trae como beneficio la disponibilidad segura del servicio aun cuando se haya presentado una incidencia en los demás dispositivos de perímetro.

8.2 ADMINISTRACIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA.

El líder de la infraestructura cuenta con unos equipos de trabajo que lo apoyaran en la actividad de mantener la infraestructura en condiciones óptimas de funcionalidad, apoyo a las exigencias de la institución, y la gestión y control de seguridad del activo de la información, contando con los siguientes equipos:

Equipo de operaciones, su actividad de conocimiento especialmente centrada al funcionamiento de la infraestructura tecnológica, supervisiones, solución de incidencias de vulnerabilidades y amenazas, y monitoreos continuos para garantizar la disponibilidad del servicio de la red.

Equipo de procesos, encargados de gestionar y mejorar la infraestructura tecnológica teniendo en cuenta un objetivo específico, su conocimiento de analistas, gestores de proyectos, y expertos en datos.

9 CONCLUSIONES

Se identifico los mínimos dispositivos de seguridad que debe tener las instituciones educativas de Colombia, para garantizar la confidencialidad, disponibilidad e integridad de la información.

Se logró describir las acciones mediante software, hardware, y de configuraciones necesarias para el endurecimiento de la seguridad de la información de las instituciones de educación media en Colombia.

Se esquematizó debidamente la topología de red con la integración de cada uno de los dispositivos esenciales, logrando el endurecimiento para la protección y efectividad de los servicios que presta la infraestructura tecnológica del centro educativo de educación media.

10 RECOMENDACIONES

Para que la seguridad de la infraestructura tecnológica y de la información en una Institución educativa de educación media sea efectiva, es esencial aplicar de manera sistemática y organizada todas las gestiones necesarias entre ellas:

- Creación de un manual donde estén definidas las políticas de seguridad, buenas prácticas, y acciones inmediatas que deben ejecutarse en caso de presentarse un ataque por parte de un ciberdelincuente.

- Involucrar en las medidas de seguridad del activo de la información a todos los usuarios de la institución, con el propósito de evitar fugas de información por errores humanos.

- Adelantar una gestión permanente de análisis de riesgos y vulnerabilidades que permitan saber el estado de la infraestructura, y la toma de decisiones tempranas en caso de presentarse amenazas.

- Fortalecimiento continuo de las acciones de seguridad de la infraestructura para evitar contratiempos que pongan en riesgo los servicios y la función de la institución.

- Establecer planes de mantenimiento tanto de dispositivos tangibles e intangibles, para la identificación de desgastes o anomalías en los sistemas que integran la infraestructura.

- Adelantar acciones continuas que estén plenamente relacionadas con la administración y manejo de la información, cumplimiento de las políticas de seguridad, y de concientización en la institución que, aunque exista una infraestructura con la mejor tecnología no quiere decir que este exenta de amenazas.

11 BIBLIOGRAFÍA

ACOMEE. [Sitio Web]. México: Router. Encaminadores en el modelo OSI. [Consulta: 17 de noviembre 2022]. Disponible en: https://www.acomee.com.mx/clasificaciones/ROUTER.pdf

AVILA, Alex, ECHEVERRÍA JIMENEZ, Tatiana. OBANDO, Christian. Y ORTIZ ZULETA, Carlos. F. [Sitio Web]. Colombia: Directrices y Política de Firewall. [Consulta: 16 de octubre 2022]. Disponible en: https://publicaciones.americana.edu.co/index.php/inam/article/view/496/654

ARUBA. A Hewlett Packard Enterprise company. [Sitio Web]. Colombia: Guía de selección para medianas empresas elige el ethernet switch más adecuado. [Consulta: 18 de octubre 2022]. Disponible en: https://www.arubanetworks.com/assets/_es/so/SLTG_SMB.pdf

CASAL PETEIRO, Manuel. [Sitio Web]. España: Arquitectura de Seguridad. [Consulta: 18 de octubre 2022]. Disponible en: http://sabia.tic.udc.es/docencia/ssi/old/2006-2007/docs/trabajos/06%20-%20Arquitecturas%20de%20Seguridad.pdf

CCIT. [Sitio Web]. Colombia: Evaluación, Retos y Amenazas de Ciberseguridad. [Consulta: 17 de octubre 2022]. Disponible en: https://www.ccit.org.co/wp-content/uploads/diagramacion-estudio-safe-evaluacion-retos-y-amenazas-a-la-ciberseguridad.pdf

CERO UNO. [Sitio Web]. México: Software Corporativo. Tipos de Arquitectura en Seguridad Perimetral. [Consulta: 16 de octubre 2022]. Disponible en: https://cerounosoftware.com.mx/2016/08/01/tipos-de-arquitectura-en-seguridad-perimetral/

ESET. [Sitio Web]. Colombia: Security Report. Latinoamérica 2020. [Consulta: 16 de octubre 2022]. Disponible en: https://www.welivesecurity.com/wp-content/uploads/2020/08/ESET-Security-Report-LATAM_2020.pdf

ESET.MAIL SECURITY. [Sitio Web]. Colombia: Protege tu servidor de correo electrónico, el vector de ataque más común. [Consulta: 14 de noviembre 2022] Disponible en: https://www.eset.com/fileadmin/ESET/ES/Docs/Fichas/Empresas/2018/ESET_Mail_Security.pdf

IBM. [Sitio Web]. España: Seguridad del correo electrónico. [Consulta: 22 de octubre 2022] Disponible en: https://www.ibm.com/docs/es/i/7.3?topic=options-e-mail-security

IDGrup. [Sitio Web]. España: ¿Qué es un Firewall y cómo funciona? [Consulta: 22 de octubre 2022]. Disponible en: https://idgrup.com/firewall-que-es-y-como-funciona/

INCIBE. [Sitio Web]. España: Almacenamiento en la nube. Políticas de seguridad para pyme. [Consulta: 11 de noviembre 2022]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/almacenamiento-nube.pdf

INCIBE. [Sitio Web]. España: Copias de seguridad. Una guía de aproximación para el empresario. [Consulta: 11 de noviembre 2022]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/guia-copias-de-seguridad.pdf

INCIBE. [Sitio Web]. España: Qué es una DMZ y cómo te puede ayudar a proteger tu empresa. [Consulta: 13 de noviembre 2022]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/dmz-y-te-puede-ayudar-proteger-tu-empresa

INCIBE. [Sitio Web]. España: ¿Qué son y para qué sirven los SIEM, IDS e IPS?. [Consulta: 13 de noviembre 2022]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/son-y-sirven-los-siem-ids-e-ips

COOLMOD. [Sitio Web]. España: Artesanos del Gaming. [Consulta: 13 de noviembre 2022]. Disponible en: https://www.coolmod.com/zyxel-gs1900-24-l2-24p-gigabit-switch/

Senado. [Sitio Web]. Colombia: Constitución Política de Colombia 1991 art. 15, p, 3. [Consulta: 25 de octubre 2022]. Disponible en: https://www.senado.gov.co/images/Archivospdf/elsenado/Normatividad/constitucion_politica.pdf

CORTES BORRERO, Rodrigo. [Sitio Web]. Colombia: Estado Actual de Política Pública de Ciberseguridad y Ciberdefensa en Colombia. Universidad de los Andes Facultad de Derecho. Rev. Derecho Común Nuevas Tecnologías. Colombia. [Consulta: 25 de octubre 2022]. Disponible en: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjVxoSBper6AhU_VTABHaVGBnkQFnoECAoQAQ&url=https%3A%2F%2Fdialnet.unirioja.es%2Fdescarga%2Farticulo%2F7496888.pdf&usg=AOvVaw2V5plTbNVOc3ladax9inn9

DELL. [Sitio Web]. EE.UU: Servidores en rack PowerEdge. [Consulta: 19 noviembre 2022]. Disponible en: https://www.dell.com/es-co/dt/servers/poweredge-rack-servers.htm#tab0=0&tab1=0&accordion0

FERNANDEZ, Lorena. [Sitio Web]. California: RZredeszone. Control de acceso: qué es y cómo ayuda a proteger nuestros datos. [Consulta: 16 noviembre 2022]. Disponibles en: https://www.redeszone.net/tutoriales/seguridad/control-de-acceso-que-es/

FORCEPOINT. [Sitio Web]. Colombia: Cortafuegos de última generación. Modelo NGFW. [Consulta: 16 noviembre 2022]. Disponible en: https://www.forcepoint.com/appliance/forcepoint-ngfw-appliances

FRESHWORKS. [Sitio Web]. EE. UU: Equipo de TI. Todo lo que necesita saber sobre los equipos de TI. [Consulta: 9 noviembre 2022]. Disponible en: https://freshservice.com/latam/equipo-ti/

GONZALEZ. (2011). Citado por FIGUEROA SUAREZ, Juan, A; RODRIGUEZ ANDRADE, Richard, F; BONE OBANDO, Cristóbal, C; y SALTOS GOMEZ, Jazmín, A. [Sitio Web]. Alemania: La seguridad informática y la Seguridad de la información. [Consulta: 18 octubre 2022]. Disponible en: https://polodelconocimiento.com/ojs/index.php/es/article/view/420/pdf

GONZALEZ HERNANDEZ, Mauricio. [Sitio Web]. Colombia: Actualidad de Colombia en Seguridad Informática. Universidad Piloto de Colombia. [Consulta: 20 octubre 2022]. Disponible en: http://polux.unipiloto.edu.co:8080/00001886.pdf

HERNANDEZ SAMPIERI, Roberto, HERNANDEZ COLLADO, Carlos, BAPTISTA LUCIO, Pilar. [Sitio Web]. México: Metodología de la Investigación. Sexta Edición, Editorial Mexicana, Reg. Número 736 México D.F., p, 152. [Consulta: 22 octubre 2022] Disponible en: https://www.uca.ac.cr/wp-content/uploads/2017/10/Investigacion.pdf

HERNANDEZ SAMPIERI, Roberto, MENDOZA TORRES, Christian. [Sitio Web]. México: Metodología de la Investigación. Primera Edición. Editorial Mexicana Reg. No. 736. México D.F., p,215. [Consulta: 22 octubre 2022]. Disponible en: https://dariososafoula.files.wordpress.com/2017/01/metodologia_de_la_investigacion_5ta_edicion-1.pdf

HewlettPackard Enterprise. [Sitio Web]. España: Seguridad en Infraestructura. ¿Qué es la seguridad en infraestructura?. [Consulta: 20 noviembre 2022]. Disponible en: https://www.hpe.com/es/es/what-is/infrastructure-security.html

HOSTALIA. [Sitio Web]. Vizcaya España: Utilización de contraseñas seguras, una acción prioritaria. [Consulta: 20 noviembre 2022]. Disponible en:

https://static.hostalia.com/news/junio11/WP_Hostalia_utiliza-contrasena-segura.pdf

Ing. DEYMONNAZ, Pablo, A. KELMAN, Uriel. UBAfiuba. Taller de Programación I Arquitectura Cliente-Servidor y Protocolo HTTP [Sitio Web]. Buenos Aires Argentina: Facultade Ingeniería. [Consulta: 16 noviembre 2022]. Disponible en: https://taller-1-fiuba-rust.github.io/clases/cliente_servidor.pdf

Ing. ROMERO ROA, Luis, F. [Sitio Web]. Colombia: Seguridad Informática en Colombia. Universidad Piloto de Colombia. Bogotá D.C. [Consulta: 20 octubre 2022]. Disponible en: http://polux.unipiloto.edu.co:8080/00047122.pdf.

INTEGO. [Sitio Web]. España: Política de contraseñas y seguridad de la información. [Consulta: 23 noviembre 2022]. Disponible en: https://www.unirioja.es/servicios/si/seguridad/concienciacion/politica_contrasenas.pdf

Kaufman y Rodríguez (1993). Citado por MORALES, Oscar. [Sitio Web]. Venezuela: Fundamento de la Investigación Documental y la Monografía. Facultad de Odontología. Venezuela., p,2. [Consulta: 13 octubre 2022]. Disponible en: http://www.saber.ula.ve/bitstream/handle/123456789/16490/fundamentos_investigacion.pdf;jsessionid=545A576CFFC564B2FE84C2FF58B196E4?sequence=1

Laudon, K. C. y Laudon, J. P. (2012) y Saroka, R. H. (2002). Citado por SISTI María Agustina (2019). Trabajo de Investigación, Seguridad Informática: La Protección de la Información en Una Empresa Vitivinícola de Mendoza., p, 40. [Sitio Web]. Mendoza Argentina, 2019. [Consulta: 13 octubre 2022]. Disponible en: https://bdigital.uncu.edu.ar/objetos_digitales/15749/sistimariaagustina.pdf

MINTIC. [Sitio Web]. Colombia: Guía No. 21. Seguridad y Privacidad de la Información. Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. [Consulta: 13 octubre 2022]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

MOLINA C. Carlos Eduardo. [Sitio Web]. EE. UU: Fundamentos de Redes. Topologías de Red. [Consulta: 13 octubre 2022]. Disponible en: http://www.redtauros.com/Clases/Fundamentos_Redes/02_Topologia_de_Red.pdf

PALOALTO. [Sitio Web]. California EE. UU: ¿Qué es un firewall virtual?. [Consulta: 13 noviembre 2022]. Disponible en: https://www.paloaltonetworks.lat/cyberpedia/what-is-a-virtual-firewall

PANDORAFMS. [Sitio Web]. Madrid: Las 16 mejores herramientas de monitoreo de Redes. [Consulta: 9 noviembre 2022]. Disponible en: https://pandorafms.com/blog/es/herramientas-de-monitoreo-de-redes/

PETI (2019-2022). [Sitio Web]. Colombia: La educación es para todos. Mineducación. Plan Estratégico de Tecnologías de la información. [Consulta: 9 octubre 2022]. Disponible en: https://www.mineducacion.gov.co/1780/articles-409158_recurso_26.pdf

QUINTERO MARTINEZ, Manuel, I. y TOVAR BALDERAS, Sergio A. [Sitio Web]. España: TiES Revista de Tecnología e Innovación en Educación Superior. Monitorización de Infraestructura Tecnológica como mejora en Centro de Datos., p,3. [Consulta: 15 noviembre 2022]. Disponible en: https://www.ties.unam.mx/num03/pdf/Monitorizacion.pdf

REVISTA INGE CUC. [Sitio Web]. Colombia: Modelo de detección de intrusiones en sistemas de red, realizando selección de características con FDR y entrenamiento y clasificación con SOM. [Consulta: 15 noviembre 2022]. Disponible en: https://revistascientificas.cuc.edu.co/ingecuc/article/view/225/214

ROCHA HARO, Cristhian A. [Sitio Web]. Ecuador: Revista Ciencia Unemi. La Seguridad Informática. Universidad Estatal de Milagro. Ecuador. [Consulta: 9 noviembre 2022]. Disponible en: https://www.redalyc.org/pdf/5826/582663867004.pdf

ROMERO CASTRO, Martha I; FIGUEROA M. Grace Liliana: VERA N. Denisse Soraya; ALAVA C. José Efraín; PARRALES A. Galo Roberto; ALAVA M. Christian José; Murillo Q. Ángel Leonardo y CASTILLO M. Mirian Adriana. [Sitio Web]. España: Ingeniería y Tecnología. 3Ciencias. Introducción a la Seguridad Informática y el Análisis de Vulnerabilidades., p,3. [Consulta: 9 noviembre 2022]. Disponible en: https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

ROSALES MONTALBAN, Eduardo, A., MARTELO GOMEZ Raúl, J., y FRANCO BORRE D.A. [Sitio Web]. Colombia: Diseño de un Sistema de Gestión de Seguridad de la Información para el Proceso de Gestión de la Infraestructura Tecnológica de Instituciones académicas Basado en Magerit. [Consulta: 16 noviembre 2022]. Disponible en: https://revistas.curn.edu.co/index.php/aglala/article/view/1579/1120.

TIES. [Sitio Web]. México: Revista de Tecnología e Innovación en Educación Superior. Gestión de la Infraestructura de TI. [Consulta: 16 noviembre 2022]. Disponible en: https://www.ties.unam.mx/num03/pdf/Gestion_de_infraestructura_de_TI.pdf

TORRES MARTINEZ, Miguel A. DLP: Prevención De Fuga De Información (Data Loss Prevention). Universidad Piloto de Colombia. Especialización en seguridad informática. [Sitio Web]. Bogotá D.C. Colombia. [Consulta: 16 noviembre 2022]. Disponible en: http://polux.unipiloto.edu.co:8080/00002325.pdf

TRENDNET. [Sitio Web]. EE. UU: Router empresarial Gigabit multi-WAN VPN. . [Consulta: 16 noviembre 2022]. Disponible en: https://www.trendnet.com/langsp/products/business-router/gigabit-multi-wan-vpn-business-router-TWG-431BR

VELASCO MELO, Arean H. [Sitio Web]. Barranquilla Colombia: Revista de Derecho. Universidad del Norte Colombia. El Derecho Informático y La gestión de la Seguridad de la Información Una Perspectiva con Base en la Norma ISO 27001. . [Consulta: 13 de octubre 2022]. Disponible en internet: https://www.redalyc.org/pdf/851/85102913.pdf

VERDEJO ALVAREZ, Gabriel. [Sitio Web]. España: “Capítulo 3: Seguridad En Redes IP: IDS”. [Consulta: 13 de octubre 2022]. Disponible en: https://www.cs.upc.edu/~gabriel/files/DEA-es-3IDS.pdf

VILLARREAL, Cesar. [Sitio Web]. EE.UU: Perfiles y sus funciones en proyectos de TI. [Consulta: 13 de octubre 2022]. Disponible en: https://www.northware.mx/blog/perfiles-y-sus-funciones-en-proyectos-de-ti/

WORPRESS. [Sitio Web]. EE. UU: Introducción a los servidores. [Consulta: 10 de noviembre 2022]. Disponible en: https://ingjpasuagrm.files.wordpress.com/2018/04/introduccion-servidores.pdf