ESPECIALIZACION EN CIBERSEGURIDAD

Diseñar una Arquitectura de Ciberseguridad Para la IPS Calculaser S.A Basada en un Inventario de Activos de Información y un Proceso de Gestión de Riesgos de Seguridad de la Información

ALEJANDRO GÓMEZ RESTREPO

ANDRÉS MAURICIO VARGAS GIL

DIEGO ALEJANDRO RÍOS HERRERA

JUAN FELIPE TRUJILLO TORO

Universidad® Católica de Manizales

VIGILADA MINEDUCACIÓN

Obra de Iglesia de la Congregación

Hermanas de la Caridad Dominicas de La Presentación de la Santísima Virgen

DISEÑAR UNA ARQUITECTURA DE CIBERSEGURIDAD PARA LA IPS CALCULASER S.A. BASADA EN UN INVENTARIO DE ACTIVOS DE INFORMACIÓN Y UN PROCESO DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN.

Trabajo de grado presentado como requisito para optar al título de *Especialista en Ciberseguridad*

Modalidad de grado: *Monografía*

Asesor

Héctor Roberto Gordon

Autores

Alejandro Gómez Restrepo
Andrés Mauricio Vargas Gil
Diego Alejandro Ríos Herrera
Juan Felipe Trujillo Toro

UNIVERSIDAD CATÓLICA DE MANIZALES
FACULTAD DE INGENIERIA Y ARQUITECTURA
ESPECIALIACION EN CIBERSEGURIDAD
MANIZALES, CALDAS
2023

Nota de aceptación 4.6

Dedicatoria

“A cada uno que impregnó un poco de sí en cada línea”

Agradecimientos

“A todas nuestras familias por permitirnos el tiempo para aprender el maravilloso mundo de la ciencia y la tecnología.”

I. Tabla de Contenido

II. Listado de tablas

III. Listado de figuras

IV. Listado de anexos

V. Listado de abreviaturas

A continuación, se presentan las abreviaturas utilizadas:

Abreviatura	Término
ISO	Organización internacional de estandarización
IDS	Sistema de detección de intrusos
IPS	Sistema de prevención de intrusos
VPN	Red privada virtual
DMZ	Zona desmilitarizada
WAN	Red de área amplia
EDR	Detección y respuesta de punto final
IA	Inteligencia artificial
SD-WAN	Redes definidas por software
SSL	Capa socket seguro
NGFW	Firewall de nueva generación
MFA2	Doble factor de autenticación
DPI	Detección profunda de paquetes
DoS	Ataque de denegación de servicio
DDoS	Ataque de denegación de servicio distribuido
BEC	Ataque que correo empresarial

Resumen

Diseñar una arquitectura de ciberseguridad para la IPS Calculaser S.A basada en un inventario de activos de información y un proceso de gestión de riesgos de seguridad de la información.

Autores: Gómez Restrepo, Alejandro.

Ríos Herrera, Diego Alejandro.

Trujillo Toro, Juan Felipe.

Vargas Gil, Andrés Mauricio.

***Palabras claves*:** Ciberseguridad, Sistema de Gestión de seguridad de la información, activo de información, gestión del riesgo, ciberdelincuentes

Contenido: El ciberespacio es el nuevo lugar donde actualmente residen la gran mayoría de las compañías. Allí interactúan, realizan transacciones de todo tipo, flujos de dinero virtual, intercambio de datos, y conviven con los cibernautas. El ciberespacio es un mundo no físico que, a semejanza del mundo real, tiene aspectos que involucran a las compañías allí presentes.

Protegerse de los ciberdelincuentes, es una labor que deben llevar a cabo día a día las compañías presentes en el ciberespacio.

Infinidad de técnicas son desarrolladas para elaborar minuciosos planes de ciberataques, y es que el avance de la tecnología ha permitido mejorar los ataques en el ciberespacio, a lo que conlleva a las compañías a mantener en constante vigilancia, a crear una postura de ciberseguridad, permitiendo protegerse de manera eficaz.

Abstract

Design a cybersecurity architecture for IPS Calculaser S.A based on an inventory of information assets and an information security risk management process.

Authors: Gómez Restrepo, Alejandro.

Ríos Herrera, Diego Alejandro.

Trujillo Toro, Juan Felipe.

Vargas Gil, Andrés Mauricio.

***Keys words*:** Cybersecurity, information security management system, information asset, risk management, cybercriminals.

Content: Cyberspace is the new place where the vast majority of companies currently reside. There they interact, carry out transactions of all kinds, virtual money flows, exchange data, and coexist with cybernauts. Cyberspace is a non-physical world that, like the real world, has aspects that involve the companies present there.

Protecting themselves from cybercriminals is a task that companies present in cyberspace must carry out every day.

Countless techniques are developed to elaborate detailed plans of cyber-attacks, and the advancement of technology has allowed to improve attacks in cyberspace, which leads companies to maintain constant vigilance, to create a cybersecurity posture, which allows them to protect themselves effectively.

Introducción

Calculaser S.A. es una institución prestadora de servicios de Salud (IPS) de tercer nivel de complejidad que presta sus servicios en el campo de la urología especializada y cuya zona de influencia comprende los departamentos de Risaralda, Quindío y Norte del Valle, cuenta hoy con más de 25 años de experiencia y reconocimiento en el mercado regional por su liderazgo en el manejo de la patología litiásica renal, del aparato reproductivo y las vías urinarias.

Respalda la prestación de los servicios con una infraestructura física, tecnológica y de recursos humanos con los más altos niveles de calidad y efectividad que buscan mejorar la calidad de vida de nuestros usuarios, así como, el cumplimiento de los requisitos establecidos bajo el marco legal del Sistema Obligatorio de Garantía de la Calidad en Salud, con procesos centrados en el usuario y una atención en salud segura.

En sus repositorios y bases de datos custodia aproximadamente 97.000 historias clínicas, del mismo número de pacientes, con un número de 300.000 folios, con 267.000 ingresos a la institución, de igual forma reposa toda la información contable, financiera, administrativa y de recursos humanos de los más de 25 años que lleva en operación, se gestiona información confidencial de alta criticidad de manejo reservado y en muchos casos con protección en custodia.

En cuanto a la evolución tecnológica, se han presentado los siguientes hitos:

- Desde su inicio en 1997 y durante los primeros años todos los procesos se realizaron de forma manual.

- En el año 2001 se implementó el primer software de gestión de historias clínicas llamado “Sahico” del proveedor Technologies Of Colombia y APOLO como software de gestión financiera, todo esto se implementó OnPremise
- En el año 2008 se implementó un servidor de archivos (Zeus) para compartir información a través de una publicación del servidor en internet sin ningún tipo de seguridad
- En el año 2014 se implementó un nuevo sistema de gestión médica llamado ISalud del proveedor GI+D
- En el año 2015 se implementó la primera solución de firewall de software libre (endian firewall) para crear una red DMZ y no exponer de forma directa el servidor de archivos y se implementó un nuevo sistema de gestión financiera y contable llamada “Yeminus”
- En el año 2017 se implementó la solución de telefonía IP y Contact Center de IKono Telecomunicaciones
- En el año 2020 se realizaron algunas implementaciones importantes como
- Se migró de la versión gratuita de correo de google y se contrata Google Workspace
- Se adopta el uso de Microsoft 365 como herramienta de ofimática
- En este mismo año inicia el despliegue de soluciones de seguridad perimetral del fabricante Sophos para la sede administrativa y se mejoró el modelo de seguridad y conectividad por VPN para el uso del servidor de archivos (zeus)
- En el año 2021 se implementó la seguridad perimetral de la sede asistencial mejorando la conectividad con la sede principal implementado una VPN Site to Site (sitio a sitio)
- Cada uno de estos sistemas ha generado grandes volúmenes de nueva data, procesada e indexada en bases de datos en servidores tanto internos como externos

facilitando la gestión de muchos procesos, reduciendo el uso del papel y conservado de manera práctica los resultados de procesos exigidos por ley.

Durante todos estos años se han abierto nuevas sedes y todas han requerido de infraestructura tecnológica para lograr un buen funcionamiento.

Por esto la Información en una organización de salud es un activo de pertenencia exclusiva y diariamente se enfrentan a amenazas y riesgos que proceden de diversos orígenes y los cuales afectan la información procesada, esta información no puede estar al alcance de agentes externos, procesos o personas no autorizadas por eso la importancia de implementar medidas para garantizar la disponibilidad, confidencialidad e integridad de la información.

En la actualidad los diversos sectores de interés para la nación definidos en el CONPES 3853, están en procesos de transformación digital, lo cual se vio acelerado por la declaración de emergencia sanitaria por COVID-19 en marzo de 2020, logrando en muy poco tiempo que las tecnologías de la información tuvieran un giro de 180 grados, generando un crecimiento exponencial en la adopción de nuevos modelos de negocio basados en los medios digitales, de igual manera se vio un aumento en la capacidad y especialización de los ciberatacantes para explotar vulnerabilidades a los sistemas de información.

Los beneficios de la era digital trae como consecuencia una serie de riesgos que pueden afectar el desarrollo normal de las actividades y generar pérdidas de información sensible y reputacional, por ello se hace necesario contar con los mecanismos de control adecuados, ya que mientras los usuarios naveguen en la Internet y no se tenga la suficiente concientización a los riesgos expuestos, otras personas malintencionadas desarrollan estrategias para acceder de forma ilegal a la información y a los recursos depositados en la

red, desarrollando programas maliciosos y virus para aprovechar las vulnerabilidades de las infraestructuras tecnológicas.

Sin importar su tamaño, todas las organizaciones pueden sufrir ataques, siendo las organizaciones con menores protocolos de protección las más expuestas y con una probabilidad muy alta de sufrir un incidente. Además, no contar con medidas de defensa adecuadas, incrementa las posibilidades de sufrir pérdidas o daños a su información.

4. Objetivos

4.1 Objetivo General

- Diseñar Una Arquitectura de Ciberseguridad Para La IPS Calculaser S.A Basada En Un Inventario De Activos De Información y Un Proceso De Gestión De Riesgos De Seguridad De La Información

4.2 Objetivos específicos

- Elaborar un inventario de activos de información con énfasis en hardware, software y servicios tecnológicos basado en la norma ISO 27001:2013.
- Realizar el proceso de gestión de riesgo para los activos de información basado en la norma ISO 27005:2011.
- Diseñar la arquitectura de ciberseguridad basada en los planes de acción técnicos derivados del tratamiento de riesgos

5. Descripción del Problema

En la actualidad, tener una postura en ciberseguridad se ha convertido en una necesidad de incluirla en los planes estratégicos de las organizaciones, debido a que los ataques informáticos pueden traer graves consecuencias en la confidencialidad, integridad y disponibilidad de la operación de estas.

Es por esto, que implementar una arquitectura en ciberseguridad permite detectar y mitigar las brechas de seguridad de la información, tanto a nivel de soluciones informáticas, de comunicaciones como de datos y de tal manera que se pueda actuar de manera preventiva para contrarrestar los ciberataques.

La definición de un protocolo (o postura) en ciberseguridad, refiere a la capacidad de una organización para defenderse de las amenazas cibernéticas, además de ser un indicador clave de la capacidad para proteger sus activos de información. Implicando el control de amenazas y vulnerabilidades, buscando minimizar los riesgos.

la implementación de políticas, procedimientos, identificación y revisión permanente de las amenazas y vulnerabilidades y el establecimiento de controles para garantizar que los riesgos no se materialicen.

Además, implica el establecimiento de una cultura organizacional en ciberseguridad, con la adecuada comprensión y adopción de todos los colaboradores, entendimiento la importancia que tiene el actuar de cada uno de estos al usar las herramientas tecnológicas y su responsabilidad de proteger los sistemas informáticos y la información.

Las empresas dedicadas a la prestación de servicios del sector de la salud, manejan información sensible y confidencial de sus pacientes, tanto a nivel de Historia Clínica como de

datos personales, seguros médicos y demás, información que para los delincuentes cibernéticos es sumamente valiosa, ya que puede ser utilizada para llevar a cabo extorsiones, fraudes y otra serie de actividades delictivas, lo que llevaría a tener consecuencias graves como lo es la pérdida de información, violación de la privacidad, pérdida de confianza de los usuarios y violación de las leyes de protección de datos, que puede tener impacto legal y financiero en las empresas.

Entre los tipos de ciberataques más comunes en el sector salud en Colombia están el phishing, el malware, el ransomware, la suplantación de identidad y además, se ha observado un aumento en el uso de malware específicamente diseñado para atacar sistemas como los de la salud, como el malware Ryuk, variante especial del ransomware.

Para protegerse de estos ataques, las empresas de servicios de salud deben con base en la identificación de los activos informáticos críticos y los riesgos, implementar una postura de ciberseguridad fuerte, que garantice la disponibilidad, confidencialidad y la integridad de los activos de información. Es por eso que Calculaser es consciente del riesgo en el que se encuentra su infraestructura tecnológica.

6. Planteamiento del Problema

Mantener una postura sólida en ciberseguridad es importante para proteger los activos críticos de la organización y asegurar la continuidad del negocio en caso de un ataque informático, para lo cual debe estar muy establecido el plan de contingencias y de recuperación de desastres.

Las empresas de servicios de salud se enfrentan continuamente a riesgos en relación con la seguridad informática, siendo sus pilares principales la confidencialidad, la disponibilidad y la integridad.

Una postura sólida en ciberseguridad se basa en varios aspectos, incluyendo:

6.1 Gestión de Activos

La gestión de activos de información se refiere a la administración y control de los recursos de información de una organización, como infraestructura tecnológica, datos, documentos, registros y otros contenidos digitales.

Su objetivo principal es maximizar el valor de estos activos y minimizar los riesgos asociados a su uso y almacenamiento.

6.2 Gestión de Riesgos

Las organizaciones deben tener procesos efectivos de gestión de riesgos para identificar, evaluar y mitigar los riesgos basados en amenazas y vulnerabilidades

6.3 Tecnologías

Las organizaciones deben utilizar tecnologías de seguridad efectivas, como antivirus con tecnologías de EDR (detección y respuesta temprana), caza de amenazas, firewalls de nueva generación (NGFW), firewall de aplicaciones web (WAF), protección de plataformas de correo electrónico y colaboración y otras soluciones, para proteger sus activos de información.

Debido a los múltiples riesgos y amenazas generados por el dinamismo enmarcado por la evolución constante de las tecnologías de la información, se hace necesario e indispensable que Calculaser adopte una postura sólida de ciberseguridad, basada en los riesgos, la evaluación de su impacto y alineada con las necesidades definidas en el direccionamiento estratégico de la entidad.

7. Justificación

Cada día hay más conciencia de la importancia de la ciberseguridad en las organizaciones, sin importar su tamaño, sector de la economía o rol que desempeña dentro de la sociedad. Todas, deben tener una postura de ciberseguridad que garantice la disponibilidad, la integridad y la confidencialidad.

Según el estándar internacional ISO 27002 “La información es un activo que, como otros activos comerciales importantes, es esencial para el negocio y en consecuencia necesita ser protegido adecuadamente. Esto es especialmente importante en el ambiente comercial cada vez más interconectado.”

Al Calcualser S.A adoptar este protocolo podrá ver fortalecido su esquema de ciberseguridad, implementando una arquitectura sólida que garantice la protección de la información y la continuidad del negocio, para el logro de este objetivo en el tiempo, la organización debe incluir las partidas presupuestales necesarias que garanticen la implementación de esta arquitectura

8. Marco Contextual

Calculaser S.A. Fue creada el 16 de diciembre de 1997 en la ciudad de Pereira, por un grupo de especialistas en el área de la urología e inició labores el 17 de diciembre de 1997. Posteriormente, el 19 de enero de 2004 mediante escritura pública 0000075 de notaria sexta de Pereira, se transforma en una sociedad anónima y registrada en cámara de comercio el 23 de marzo de 2004

En el transcurso de los años y con la experiencia de más de 25 años se ha venido posicionando como una institución que lidera los avances tecnológicos y la integración de la tecnología de punta con los conocimientos técnicos y científicos de los profesionales vinculados a la institución. Actualmente como IPS de mediana complejidad, presta servicios en campo de la urología especializada para su zona de influencia Pereira y Armenia, cuenta con 5 sedes de las cuales 4 son asistenciales y la sede administrativa, sus procesos están centrados en el usuario de acuerdo con los lineamientos del ministerio de salud en materia de atención segura en salud.

Para ello integra todos los recursos disponibles y los orienta hacia el logro de los objetivos del sistema de salud de nuestro país y como consecuencia de ello se alcanzan los objetivos institucionales que permiten el reconocimiento a nivel empresarial en el sector e impulsa el crecimiento en el mercado y el respaldo de nuestros clientes.

La Organización

Calculaser S.A es una Institución Prestadora de Servicios de tercer nivel de complejidad más importante de los departamentos de Risaralda y Quindío, con una trayectoria en el mercado de la salud por más de 25 años, en el campo de la urología convencional y especializada ofreciendo los siguientes servicios:

- Cirugía cálculo renal
- Cirugía urológica
- Procedimientos urológicos diagnósticos

Direccionamiento Estratégico

Misión

Somos una institución prestadora de servicios de salud especializada en urología, consultas médicas y servicios quirúrgicos, que asegura los medios tecnológicos, humanos, físicos y métodos adecuados para la satisfacción de nuestros clientes. Así mismo, velamos por el bienestar, seguridad y competencia de nuestro talento humano, enmarcando nuestro servicio dentro del respeto por el medio ambiente y aseguramos la contratación de proveedores idóneos para prestar nuestros servicios con calidad.

Visión

Ser una institución prestadora de servicios de salud elegida en la región por la utilización y mantenimiento de tecnología de punta, la búsqueda continua de competitividad organizacional, el mantenimiento de entornos laborales saludables y el desarrollo permanente de competencias científicas de sus especialistas, incrementando así su capacidad operacional y garantizando el continuo valor de la empresa para los accionistas y para la sociedad.

Objetivos Corporativos

- Asegurar la satisfacción del usuario.
- Garantizar rentabilidad a los accionistas.
- Mejorar la competencia del talento humano.
- Permanecer a la vanguardia en tecnología.

- Tener crecimiento en el mercado regional.

Principios y Valores

Responsabilidad y Honestidad: Entendemos el papel que jugamos en la sociedad y de cómo nuestras acciones impactan en el crecimiento de nuestro país, por esta razón nuestro trabajo diario está impulsado a generar confianza en nuestra institución y en nuestra sociedad.

Perseverancia: En nuestra organización hacemos que las situaciones se conviertan en oportunidades de mejora, entendemos que hay momentos difíciles, pero que son superados gracias al equipo humano con el que contamos. Cada logro es un paso más, para trazar una nueva meta.

Políticas de Gestión Integral

Calculaser S.A. es una institución prestadora de servicios de salud, que asegura y satisface las necesidades de las partes interesadas basado en los siguientes principios:

Establecer procesos de toma de decisiones que generen valor a la organización basado en los principios establecidos en el código de ética y buen gobierno.

Cumplir con la normatividad legal vigente en el marco del SOGC, el SG-SST y el SGC.

Otras disposiciones

- Ampliar el portafolio de servicios en el área de influencia.
- Propender por una tecnología biomédica de vanguardia.
- Brindar atención basada en evidencia científica y prácticas clínicas seguras para el usuario.
- Mejorar la infraestructura de manera que genere valor agregado en la prestación del servicio

- Actualizar permanentemente la plataforma documental.
- Mantener entornos laborales saludables y seguros mediante la identificación, gestión del riesgo y el mejoramiento continuo.
- Mejorar continuamente la competencia del talento humano mediante su capacitación, formación, entrenamiento y supervisión.
- Establecer relaciones comerciales de mutuo beneficio con proveedores evaluados y seleccionados técnicamente para cumplir los procesos de manera óptima y brindar atención de calidad.

Calculaser S.A tiene definida y establecida una política de tratamiento y protección de datos personales (29) enmarcada en el cumplimiento de la Ley 1581 de 2012, Decreto 1377 de 2013, Decreto 886 de 2014, y el Decreto 090 de 2018, con el fin de garantizar la confidencialidad de la información almacenada en el Sistema de información HIS/ISalud.

La organización será descrita en las siguientes páginas a través de un conjunto de ilustraciones que brindan un mapa tecnológico general de la conformación de esta empresa.

Mapa de Procesos

En la siguiente gráfica se observa la distribución de los procesos estratégicos, misionales y de apoyo que garantizan la operación en la organización para el cumplimiento de los objetivos estratégicos.

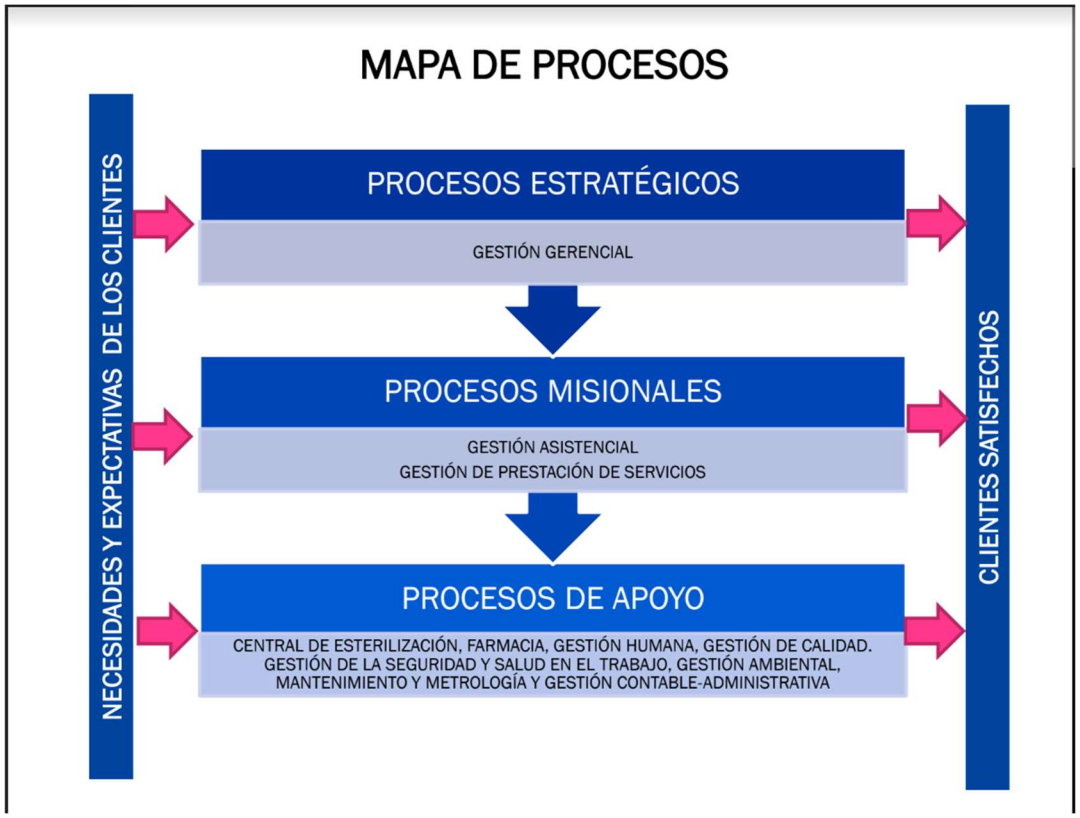


Figura 1. Mapa de procesos de la empresa Calculaser S.A

Nota. Fuente Elaboración Propia

Organigrama

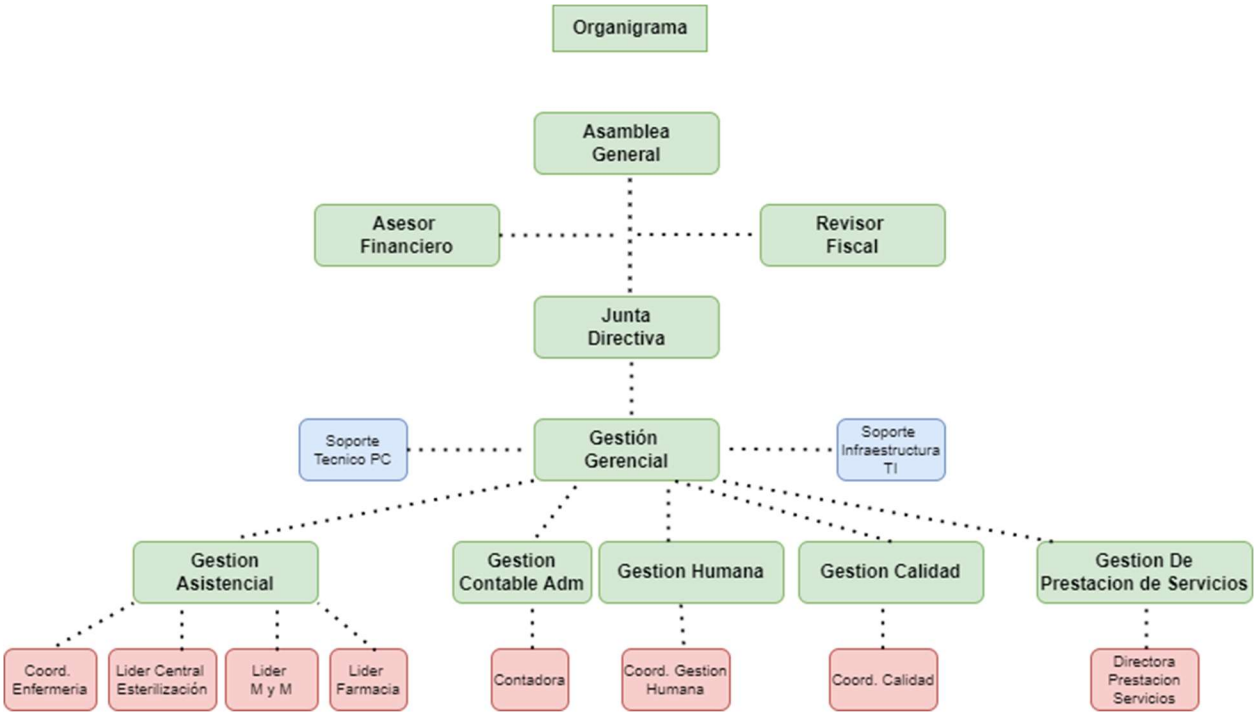


Figura 2. Organigrama de la empresa Calculaser S.A

Nota. Fuente Elaboración Propia

Sedes

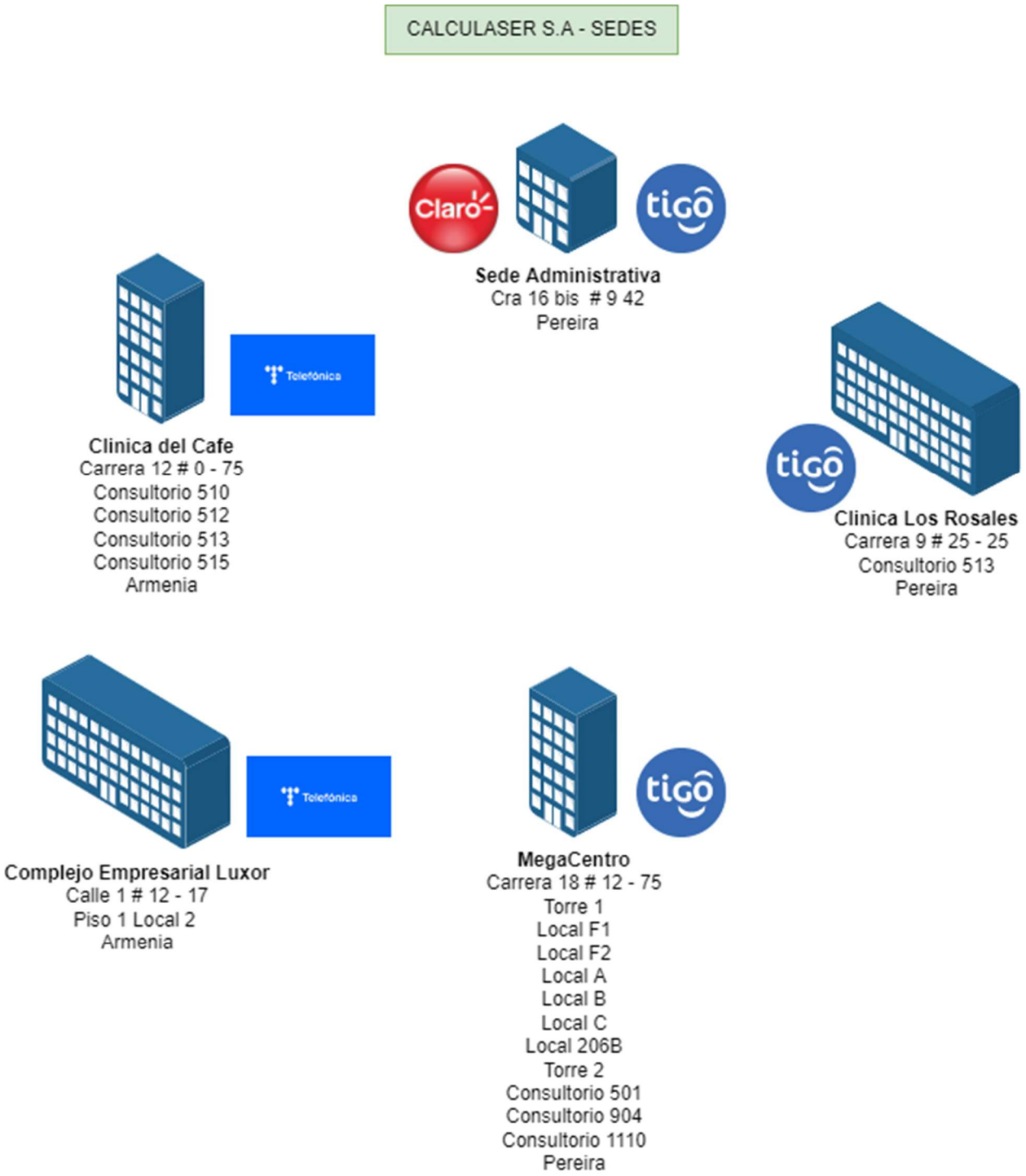


Figura 3. Sedes de la empresa Calculaser S.A

Nota. Fuente Elaboración Propia

Diagrama de Acceso a Internet y Servicios

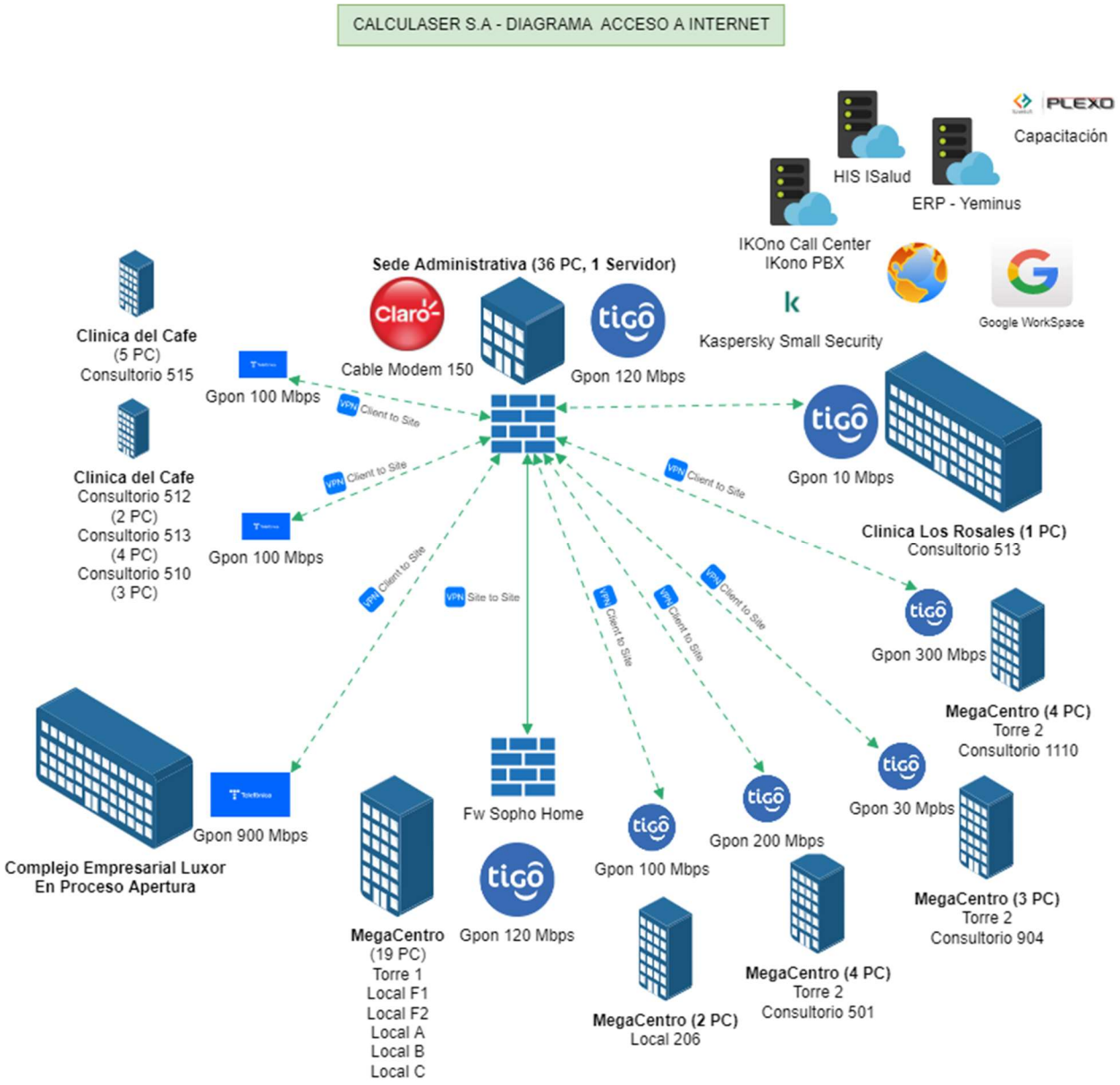


Figura 4. Conectividad y acceso a internet de la empresa Calculaser S.A

Nota. Fuente Elaboración Propia

Diagrama de Red Sede Principal

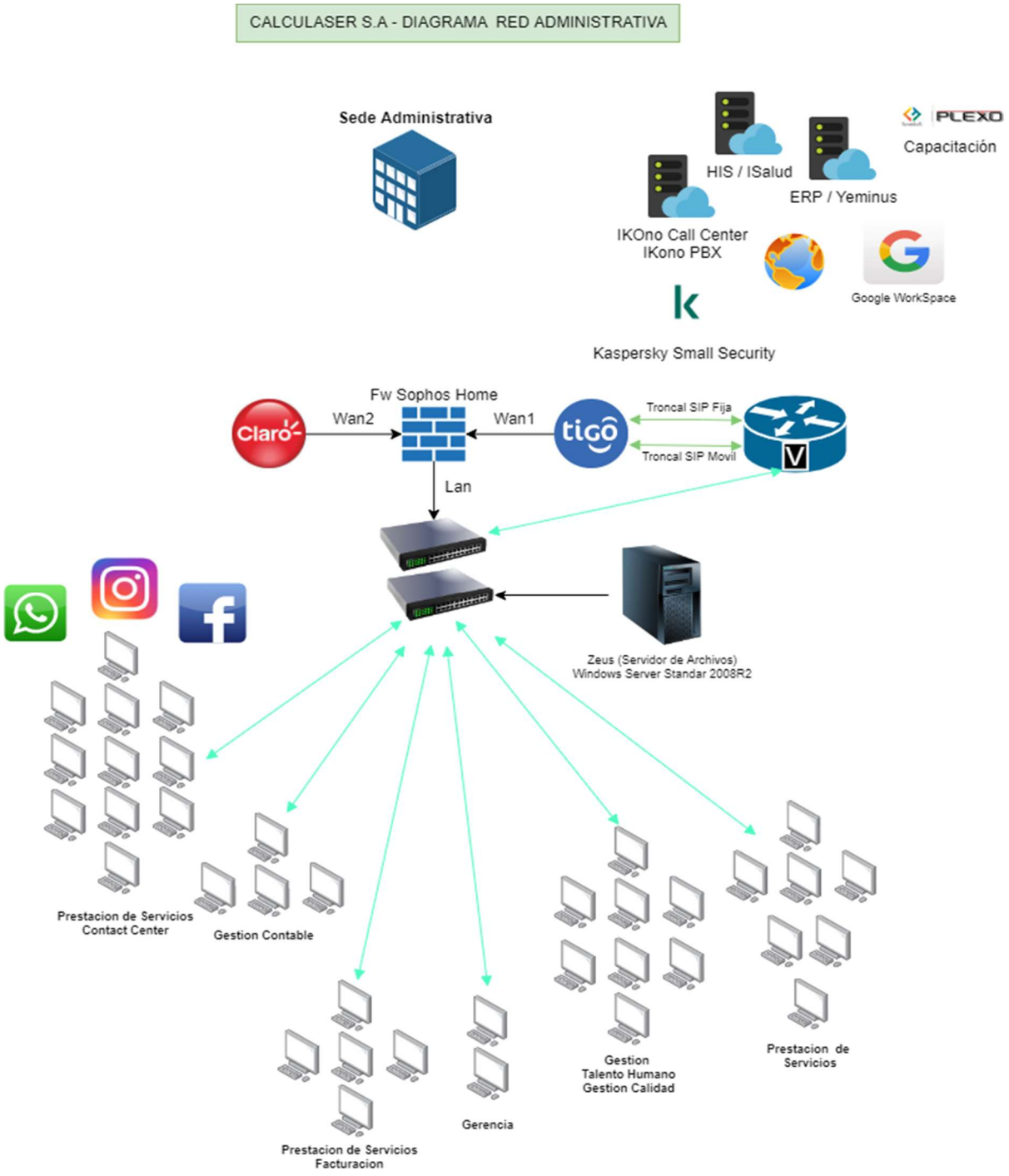


Figura 5. Diagrama de red sede principal.

Fuente Elaboración Propia

- **Ingresos Anuales**

INGRESOS ULTIMOS 3 AÑOS			
	2020	2021	2022
Calculaser S.A	$ 8.130.195.578	$ 10.603.782.061	$ 15.445.213.381

Tabla 1. Ingresos Calculaser S.A

Nota. Elaboración Propia

- **Inventario de Sedes**

Inventario de Sedes						
Sede	Descripcion	Ciudad	Dirección	Provedor Internet	Servicios	# Colaboradores
1	Administrativa	Pereira	Calle 16B # 9 - 42	TIGO y Claro	Administrativos	33
2	Asistencial	Pereira	Carrera 18 # 12 - 75 MegaCentro	TIGO	Quirurgicos	86
	Local 206B	Pereira	Carrera 18 # 12 - 75 MegaCentro	TIGO	Terapia Piso Pelvico	2
	Consultorio T2 501	Pereira	Carrera 18 # 12 - 75 MegaCentro	TIGO	Consulta Externa y Procedimientos Diagnosticos	4
	Consultorio T2 904	Pereira	Carrera 18 # 12 - 75 MegaCentro	TIGO	Consulta Externa Otras Especialidades	1
	Consultorio T2 1110	Pereira	Carrera 18 # 12 - 75 MegaCentro	TIGO	Consulta Apoyo Urologica	2
3	Consultorio 513	Pereira	Carrera 9 # 25 - 25 Clinica Rosales	TIGO	Consulta Externa	0
4	Consulorio 510	Armenia	Carrera 12 # 0 - 75 Clinica del Café	Movistar	Consulta Apoyo Urologica	7
	Consulorio 512	Armenia	Carrera 12 # 0 - 75 Clinica del Café	Movistar	Consulta Externa y Procedimientos Diagnosticos	
	Consulorio 513	Armenia	Carrera 12 # 0 - 75 Clinica del Café	Movistar	Procedimientos no Invasivos	
	Consulorio 515	Armenia	Carrera 12 # 0 - 75 Clinica del Café	Movistar	Consulta Externa y Procedimientos Diagnosticos	
5	Piso 1 Local 2	Armenia	Calle 1 # 12 - 17 Complejo Empresarial Luxor	Movistar	Consulta Externa y Procedimientos Diagnosticos	10

Tabla 2. Sedes Calculaser S.A

Nota. Elaboración Propia

8.1 Marco Demográfico

Calculaser S.A es una institución prestadora de salud que cuenta con aproximadamente 150 usuarios que interactúan diariamente con los diferentes sistemas de información y herramientas de apoyo de la entidad, el personal está distribuido de la siguiente forma 75% en el área asistencial y el otro 25% en el área administrativa

8.2 Contexto Geográfico

Como lo indica la Constitución Política de Colombia en el Título 1 denominado “De Los Principios Fundamentales”, su Artículo 1 promulgar lo siguiente:

“Artículo 1”. El estado colombiano es un estado social de derecho organizado en forma de República unitaria, descentralizada, con autonomía de sus entidades territoriales, democrática, participativa y pluralista. fundada en el respeto de la dignidad humana, en el trabajo y la solidaridad de las personas que la integran y en la prevalencia del interés general.” y la división del Estado se establece en tres ramas del poder ejecutivo, legislativo y judicial, y adicionalmente posee organismos de control independientes como la Procuraduría, Contraloría, entre otros.

Con base en la información anterior, es posible afirmar que en Colombia existe una amplia variedad de entidades en cada uno de los sectores, las cuales pueden ser diferenciadas por su función y alcance. Todas y cada una de éstas organizaciones deberían tener un esquema organizacional y una asignación presupuestal para infraestructura TI y contratación de profesionales de las TIC.

Las tecnologías de la información y la comunicación juegan un papel importante en las organizaciones, a tal grado que se consolida una oficina de T.I mediante la cual se pretende

gerenciar los servicios TI y alinearlos a los objetivos institucionales para alcanzar el cumplimiento de la misión. Para lograr tal objetivo, la oficina de tecnologías de la información o área de telecomunicaciones debe ofrecer a su organización una serie de servicios útiles y comunes a cualquier tipo de institución o sector:

- Gestión de TI
- Atención de mesa de servicio
- Sistemas de información
- Gestión de Cambios
- Provisión de equipos
- Intercambio de datos con entidades de control
- Seguridad de la información

Los servicios mencionados, a pesar de ser citados de forma independiente, al ser llevados a la práctica requieren una constante cooperación. Sin embargo, se destaca la seguridad de la información como un proceso transversal a todos los servicios, mediante el cual se garantiza el cumplimiento eficiente del objetivo de cada uno de ellos. Esto significa que la implementación de un esquema de ciberseguridad que respalde cada proceso, garantiza el uso seguro y aprovechamiento de los recursos TI, reduciendo el riesgo a sufrir pérdidas de información, daños de activos o sistemas comprometidos por cualquier tipo de ciberataque. De esta forma es posible asegurar que toda entidad en Colombia requiere contar con un grupo de profesionales TI orientados a la ciberseguridad, que, mediante conocimiento avanzado de hacking e intrusión, propongan una estrategia de seguridad efectiva a partir de la cual sea posible:

• Garantizar la integridad, disponibilidad y confidencialidad de la información.

• Establecer una categorización de los activos de información de la empresa

• Establecer una estrategia de mitigación de riesgos en materia de ciberseguridad.

• Establecer políticas de prevención y procesos que promuevan la seguridad informática en la entidad.

• Establecer un consolidado de riesgos estimados para la entidad y sus activos

• Establecer un plan de respuesta a posibles incidentes que se presenten en materia de ciberseguridad.

Gracias a las políticas de ciberseguridad que emitió el CONPES 3701 permitió generar una comisión intersectorial guiada desde algunas entidades del gobierno central como lo es el Colcert para que todas las entidades del país tanto públicas como privadas, y de todos los sectores de la economía, los cuales fueron descritos en el CONPES 3854, accedieron a la “colaboración activa en la resolución de incidentes”, de ciberseguridad.

Figura 6. Modelo de coordinación Ministerio de defensa Nacional

Nota. Fuente Ministerio de Defensa Nacional

Es así como Calculaser S.A hace parte del sector (XI) salud y protección social, (remitirse al título 9.2.1 Marco Nacional, para más información) priorizado en el CONPES 3854, siendo este uno de los sectores más afectados, afectados y vulnerados en el año 2022 en Colombia.

En caso de existir un evento de seguridad informática donde el impacto tenga niveles de severo o catastrófico y la propia organización se vea disminuida en su capacidad de reacción y atención podría acudir al modelo de coordinación descrita en la figura 6 para obtener las capacidades, técnicas, administrativas y legales que brinda el gobierno a través del colcert.

9. Marcos de la investigación

9.1 Antecedentes

En Colombia existen diferentes herramientas que brindan lineamientos de políticas, leyes y regulación para la ciberseguridad y ciberdefensa como en el documento CONPES 3701 del año 2011 o el CONPES 3854 que nos indica la política nacional de seguridad digital como en otros países, los únicos acercamientos se han planteado en el CONPES 3701:2011 política de ciberseguridad y ciberdefensa.

Desde el año 2014 todas las IPS están obligadas a manejar historias clínicas sistematizadas, las cuales deben conservar su integridad, disponibilidad y confidencialidad según normativa expedida por el ministerio de salud; bajo esta premisa la seguridad de la información en las instituciones prestadoras de salud debe garantizar.

La Universidad Piloto de Bogotá, ha abordado el estudio del estado y el manejo de la seguridad de la información en entidades de salud como es el caso de la clínica Miocardio de Bogotá, ahondando en las historias clínicas digitales y en el manejo estricto y de reservas en el cual se registran cronológicamente las condiciones de salud un paciente, los actos médicos y los demás procedimientos ejecutados por el equipo de salud que interviene en su atención, por lo cual se define un documento legal que se puede utilizar en un marco jurídico y mucho más cuando la ley colombiana así lo decreta. (Bahos, 2014).

En el artículo “DOCUMENTO CONPES 3701 LINEAMIENTOS DE POLÍTICAS PARA CIBERSEGURIDAD Y CIBERDEFENSA” publicado por Wilson Guerrero, el autor realiza un breve análisis del documento CONPES 3701, en el cual se aborda una estrategia para afrontar las diferentes amenazas, a las que se encuentran significativamente expuestas las entidades del país, mediante la inclusión del tema “ciberdefensa y ciberseguridad” en el Plan Nacional de

Desarrollo, que busca fortalecer las capacidades del estado y mitigar el impacto de dichos ataques(1).

En el ámbito intencional e la Unión Internacional de Telecomunicaciones (UIT), el Banco Mundial, la Secretaría de la Commonwealth (Comsec), la Organización de Telecomunicaciones de la Commonwealth (CTO) y el Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN (CCDCOE OTAN), desarrollaron una guía para la elaboración de una estrategia nacional de ciberseguridad

9.2 Marco Normativo

Colombia ha generado avances en su legislación un marco legal y un marco reglamentario sobre ciberseguridad y ciberdefensa, protección de datos personas y regulación sobre la historia clínica del país teniendo en cuenta aportes que datan del año 1999 hasta la actualidad y objeto de este numeral y párrafos siguientes es darlos a conocer de manera explícita, así como entender los límites de actuación en Colombia.

De esta manera podemos encontrar en el cuerpo legislativo y organizado de manera cronológica lo siguiente:

9.2.1 Marco Normativo Nacional

- ***Ley 23 de 1981 Normas en Materia de Ética Médica…*** “En su capítulo 3 desarrolla el tema de la historia clínica y habla sobre su registro, privacidad, reserva y autorización de su uso.”
- La Resolución 1995 de 1999 en el artículo 18, en relación con los medios técnicos de registro y conservación de la historia clínica

- **Constitución política de Colombia**: Artículos 11, 12, 13, 14, 17, 21, 22, 24, 29, 44, entre otros. Por ejemplo, el Art. 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.
- ***Ley 527 de 1999 Comercio Electrónico***… "Uso y acceso de los mensajes de datos, del comercio electrónico y de las firmas digitales". Hace parte del Marco Legal en él se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y firmas digitales y es usado para verificar la validez jurídica y probatoria de la información electrónica.
- ***Ley 594 de 2000***… "Ley general de archivos". Hace parte del Marco Legal.
- ***Ley 599 de 2000 Código Penal***… "Se mantuvo la estructura del tipo penal de Violación Ilícita de archivos de comunicaciones, se creó el bien jurídico de los derechos de autor y se incorpora alunas conductas con el delito informático, tale como la interceptación". Hace parte del Marco Legal. Se tipificó el "Acceso abusivo a un sistema informático en el ART.195"
- ***Ley 679 de 2001… "Pornografía Infantil"***

  Hace parte del Marco Legal usado para verificar la responsabilidad de los ISP's.

- **Ley 962 de 2005**… "Simplificación y racionalización de trámites administrativos en entidades del estado". Hace parte del Marco Legal es usado para verificar atributos de seguridad en la información electrónica de entidades públicas.

- ***Ley 1150 de 2007***… “Seguridad de información electrónica en contratación en línea, se introducen medidas de eficiencia y transparencia en la ley 80 de 1993 sobre la contratación con recursos públicos, se desarrolla el SECOP” (2). Hace parte del Marco Legal.
- ***Ley 1266 de 2008… “Habeas Data Financiera y seguridad de datos personales***
- ***Ley 1273 de 2009…” Protección de la información y de los datos”*** (3) declara: “por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".
- ***Ley 1341 DE 2009 Tecnologías de la información y aplicación de ciberseguridad.*** “Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la Información y las Comunicaciones –TIC, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.”
- ***Resolución de la Comisión de Regulación de Comunicaciones 2258 de 2009…*** ***“***Sobre seguridad de las redes de los proveedores de redes y servicios de telecomunicaciones. Esta resolución modifica los artículos 22 y 23 de la Resolución CRT 1732 de 2007 y los artículos 1,8 y 2,4 de la Resolución CRT 1740 de 2007. Esta regulación establece la obligación para los proveedores de redes y/o servicios de telecomunicaciones que ofrezcan acceso a Internet de implementar modelos de seguridad, de acuerdo con las características y necesidades propias de su red, que contribuyan a mejorar la seguridad de sus redes de acceso, de acuerdo con los marcos de seguridad definidos por la UIT, cumpliendo los principios de confidencialidad de datos, integridad de datos y disponibilidad de los elementos de red, la información, los

servicios y las aplicaciones, así como medidas para autenticación, acceso y no repudio. Así mismo, establece obligaciones a cumplir por parte de los proveedores de redes y servicios de telecomunicaciones relacionadas con la inviolabilidad de las comunicaciones y la seguridad de la información"

- ***Ley 1437 de 2011… "Procedimiento administrativo y aplicación de criterios de seguridad".***
- ***Ley 1480 de 2011… "Protección al consumidor por medios electrónicos"***

  Hace parte del Marco Legal es usado para brindar seguridad en transacciones electrónicas.

- ***CONPES 3701 2011: … "Este documento establece los Lineamientos de política para ciberseguridad y ciberdefensa"*** Publicado el 14 de Julio de 2011.
- ***Decreto Ley 019 de 2012… "Racionalización de trámites a través de medios electrónicos".***

  Hace parte del Marco Legal es usado para brindar los criterios de seguridad.

- ***Ley 1581 de 2012… "Ley estatutaria de protección de datos personales"***

  Hace parte del Marco Legal.

- ***Ley 1623 de 2013… "Ley de Inteligencia".***

  Hace parte del Marco Legal es usado para brindar los criterios de seguridad.

- ***Ley 1712 de 2014… "Transparencia en el acceso a la información Pública".***
- ***Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones".***
- ***CONPES 3854 de 2016… "Este documento establece la Política Nacional de Seguridad Digital"*** *(4)*

Este documento establece la Política Nacional de Seguridad Digital, donde en primer lugar establece un marco institucional alrededor de la seguridad digital en el gobierno, brinda conceptos básicos, modela un esquema de gestión sistemática para los riesgos de seguridad digital, además, muestra los principios fundamentales por los que se rige la política, tales como salvaguardar los derechos humanos y valores fundamentales, adopta un enfoque incluyente y colaborativo que involucra a todas las partes interesadas, asegurar una responsabilidad compartida entre las partes interesadas y adopta un enfoque basado en la gestión de riesgos. En segundo lugar, relaciona unos antecedentes de la temática, diagnosticando el estado de la ciberseguridad en el país. En tercer lugar, define la política teniendo en cuenta la gestión de riesgos, partes interesadas, fortalecimiento de la defensa generando mecanismos continuos para promover la contribución en seguridad digital a nivel nacional e internacional, adicionalmente, valora el impacto económico de la política.

A través de este instrumento público se le ordena a la policía nacional crear el Centro cibernético de la policía nacional. Ver 9.3.1.3

- ***Decreto 1008 de 2018***: "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto número 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones DUR-TIC.
- ***Resolución 500 del 10 de marzo de 2021:*** "por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital".
- ***Directiva Presidencial No. 3 del 15 de marzo de 2021:*** respecto a lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.

- ***Directiva Presidencial No. 02 del 24 de febrero de 2022:*** cuyo asunto es la reiteración de la Política Pública en materia de Seguridad Digital.

9.2.2 Marco Normativo Internacional

Los principales instrumentos internacionales en materia de ciberseguridad, ciberdefensa y protección de datos son:

Convenio de Budapest "Convenio sobre Ciberdelincuencia del Consejo de Europa – CCC (conocido como el convenio sobre cibercriminalidad de Budapest) Adoptado en noviembre de 2001 y entrada en vigor desde el 1° de julio de 2004."

El objetivo principal del convenio es la adopción de una legislación que facilite la prevención de las conductas delictivas y contribuya con herramientas eficientes en materia penal que permitan detectar, investigar y sancionar las conductas antijurídicas.

Único instrumento vinculante vigente sobre el tema en el ámbito internacional y su protocolo para la criminalización de actos de racismo y xenofobia cometidos a través de sistemas informáticos.

El Consejo considera que el delito cibernético exige una política penal común destinada a prevenir la delincuencia en el ciberespacio y en particular, hacerlo mediante la adopción de legislación apropiada y el fortalecimiento de la cooperación internacional.

Cabe resaltar que, si bien el CCC tuvo su origen en el ámbito regional europeo, es un instrumento abierto para su adhesión a todos los países del mundo.

NIST National Institute Of Standards and Technology –, ha desarrollado un marco de ciberseguridad que proporciona una guía para que las organizaciones gestionen y reduzcan el riesgo de ciberseguridad.

El marco se centra en cinco funciones principales: identificar, proteger, detectar, responder y recuperar, y se puede adaptar a las necesidades de cualquier organización, independientemente de su tamaño, sector o presupuesto.

El NIST también ha desarrollado una gran cantidad de estándares y guías relacionados con la ciberseguridad, como el Estándar de Criptografía Avanzada (AES), el Estándar de Seguridad de Datos para la Interconexión de Sistemas de Salud (HIPAA), y el Estándar de Interconexión y Seguridad en la Nube (FISMA), entre otros. Estos estándares y guías son ampliamente utilizados tanto en los Estados Unidos como en todo el mundo como referencias para la implementación de medidas de seguridad de la información y la ciberseguridad.

HIPAA significa Ley de Portabilidad y Responsabilidad del Seguro de Salud en inglés, y es una ley federal de los Estados Unidos que establece normas de privacidad y seguridad para la información médica y de salud protegida.

Esta ley se promulgó en 1996 para proteger la confidencialidad de la información médica del paciente y para garantizar la portabilidad de los seguros médicos.

Bajo HIPAA, los proveedores de atención médica, los planes de salud, los clearinghouses (procesadores de transacciones de seguros médicos) y sus asociados deben cumplir con ciertos requisitos de privacidad y seguridad para proteger la información de salud identificable personalmente (PHI, por sus siglas en inglés) de los pacientes.

Entre las disposiciones más importantes de HIPAA se encuentran las siguientes:

- Requisitos para la protección y seguridad de la PHI, incluyendo medidas físicas, técnicas y administrativas para garantizar su confidencialidad, integridad y disponibilidad.

- La necesidad de que las organizaciones firmen acuerdos de asociación de negocios para garantizar que los asociados también cumplan con los requisitos de HIPAA.
- La necesidad de obtener el consentimiento informado del paciente antes de utilizar o divulgar su PHI, con ciertas excepciones.
- El derecho del paciente a acceder y controlar su propia PHI, incluyendo el derecho a solicitar copias de su información médica y a solicitar correcciones.
- La necesidad de notificar a los pacientes en caso de una violación de la PHI.
- El incumplimiento de HIPAA puede resultar en multas y sanciones severas, por lo que es importante que las organizaciones cubiertas por esta ley implementen medidas adecuadas para cumplir con sus requisitos de privacidad y seguridad de la información médica y de salud.

Reglamento General de Protección de Datos (GPDR), es una ley de protección de datos y privacidad de los ciudadanos de la Unión Europea (UE). Entró en vigor en mayo de 2018 y sustituyó a la Directiva de Protección de Datos de la UE de 1995.

El RGPD establece un marco de protección de datos más riguroso y detallado para las empresas que recopilan y procesan datos personales de los ciudadanos de la UE.

También proporciona mayores derechos a los titulares de los datos, incluyendo el derecho a ser informados sobre cómo se están utilizando sus datos, el derecho a acceder a sus datos personales y el derecho a solicitar que se eliminen sus datos personales.

9.3 Marco Teórico Conceptual

Debido a la evolución permanente de las tecnologías de la información y las comunicaciones, lo cual demanda un mayor esfuerzo por parte de las personas y las organizaciones para garantizar seguridad ante las constantes amenazas a las que se ven expuestos los activos de información del sector salud.

De igual manera hoy en día quienes atentan contra la seguridad de la información y la ciberseguridad, utilizan herramientas y métodos más sofisticados para vulnerar activos de información y esto junto a la normatividad que emite el ente regulador en donde exige mayor protección y privacidad de los datos sensibles, personales, comerciales y financieros las organizaciones deben contar con una arquitectura de ciberseguridad basada en estándares reconocidos a nivel mundial.

Para efectos de tener claro los conceptos principales en los que se basa este trabajo de grado a continuación se describen, y en el anexo G se detallan el resto de los términos utilizados.

9.3.1 Seguridad de la Información

Son medidas preventivas que incluyen factores de confidencialidad, integridad, disponibilidad, autenticidad, responsabilidad, aceptabilidad y confiabilidad de la información.

La información representa uno de los activos más valioso de las organizaciones, lo que implica que es indispensable asegurar su protección contra amenazas y eventos que puedan llegar comprometer su confidencialidad, integridad y disponibilidad. La información puede existir en diferentes medios tanto físicos como electrónicos, pero independientemente del medio, es

necesario que las organizaciones garanticen y aseguren la debida protección de la información durante su recolección, almacenamiento, tratamiento y uso.

La seguridad de la información en una organización, es un proceso de mejora continua que demanda la participación activa de toda la organización y busca preservar, entre otros, los siguientes principios de la información:

- **La confidencialidad**: Característica de la información por medio de la cual no se revela ni se encuentra a disposición de individuos, organizaciones o procesos no autorizados
- **La disponibilidad:** Es la garantía de poder acceder a los activos de la información cuando sea necesario, por personal autorizado
- **La integridad:** La propiedad de salvaguardar la exactitud y completitud de los activos de información.
- **Amenaza, riesgo y vulnerabilidad:** En el ámbito de la ciberseguridad, podemos definir el riesgo como la probabilidad de que ocurra un incidente de seguridad, como el riesgo no es más que una probabilidad, se puede medir y se suele cuantificar, por otro lado, la amenaza es una acción que podría tener un potencial efecto negativo sobre un activo. Es decir, una amenaza es cualquier cosa que pueda salir mal. Hay que tener en cuenta que una amenaza por sí misma no provoca un daño, pero podría provocarlo. Las amenazas se comprenden mejor si se clasifican atendiendo a cómo pueden dañar a un activo: esencialmente, pueden afectar a su disponibilidad, a su confidencialidad o su integridad.

> Para que se produzca un daño es necesario que exista una debilidad o fallo en el sistema que permita que se materialice una amenaza. Estas debilidades, fallos o “huecos de seguridad” son las vulnerabilidades, que pueden ser de diferente naturaleza, de diseño, de arquitectura y configuración, de estándares de uso y procedimientos, etc. Es decir, cuando se dice que un activo es vulnerable, significa que tiene un agujero que puede ser aprovechado para provocar un incidente de seguridad.

9.3.2 Normas ISO/IEC 27000

La familia de las normas ISO/IEC 27000, son un marco de referencia de seguridad a nivel mundial desarrollado por la International Organization for Standardization - ISO e International Electrotechnical Commission – IEC, que proporcionan un marco, lineamientos y mejores prácticas para la debida gestión de seguridad de la información en cualquier tipo de organización.

Estas normas especifican los requerimientos que deben cumplir las organizaciones para establecer, implementar, poner en funcionamiento, controlar y mejorar continuamente un Sistema de Gestión de Seguridad de la Información.

En Colombia, el Instituto Colombiano de Norma Técnicas y Certificaciones, ICONTEC, es el organismo encargado de normalizar este tipo de normas.

Las siguientes son algunas de las normas que componen la familia ISO/IEC 27000, las cuales serán el marco teórico que se tendrá en cuenta para efectos del presente trabajo:

- **ISO/IEC 27001:2013** Es una norma internacional que establece los requisitos para un sistema de gestión de seguridad de la información (SGSI). Esta norma

es aplicable a cualquier tipo de organización, independientemente de su tamaño, naturaleza o sector, que busque proteger su información mediante la implementación de controles de seguridad adecuados.

- **ISO/IEC 27005:2011** Es una norma internacional que proporciona directrices para la gestión del riesgo de seguridad de la información. Esta norma es compatible con los conceptos generales especificados en ISO/IEC 27001 y está diseñada para ayudar a la implementación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.

- **ISO/IEC 27032:2012** proporciona directrices para mejorar el estado de la ciberseguridad, destacando los aspectos únicos de esa actividad y sus dependencias en otros dominios de seguridad, en particular: seguridad de la información, seguridad de redes, seguridad en Internet y protección de infraestructuras críticas de información.

9.3.3 CheckPoint

Es una empresa de ciberseguridad que ofrece soluciones avanzadas para proteger las redes y los datos de las organizaciones. Sus soluciones se centran en la prevención proactiva de amenazas cibernéticas y utilizan tecnologías avanzadas para detectar y prevenir amenazas en tiempo real.

A continuación, se describen una serie de actores nacionales, estadísticas, empresas afectadas, colectivos y tipos de ataques mas comunes en el ambito local y internacional:

9.3.4 Entidades Asociadas con Ciberseguridad en Colombia

En el caso colombiano contamos con diferentes articuladores en la protección de las ICC (Infraestructuras Críticas Cibernéticas). En la cabeza de la coordinación se encuentra la Presidencia de la República, entidades y ministerios que apoyan las responsabilidades como el MinTIC, MinJusticia, Cancillería, la Dirección Nacional de Inteligencia, el Departamento Nacional de Planeación, la Unidad de Información y Análisis Financiera y la Fiscalía General de la Nación.

Sin embargo, los implicados de manera directa en la ciberseguridad y ciberdefensa del país son en especial tres organismos:

(i) el ColCERT,
(ii) el Comando Conjunto Cibernético (CCOCI) y
(iii) el Comando Cibernético Policial (CCP).

Estos tres están encargados de la protección de los activos IT y OT de los 13 sectores en Colombia, el ColCERT como coordinador a nivel nacional en la ciberseguridad de las ICC [5], el CCOCI como unidad militar con componentes conjuntos y coordinador de las Fuerzas Militares, es el principal organismo en la protección y ciberdefensa de ICC y el CCP como cuerpo encargado de la ciberseguridad ciudadana y la judicialización del cibercrimen.

Adicionalmente a lo anterior, en Colombia contamos con CSIRTs específicos que aportan al monitoreo de seguridad digital en algunos sectores; a pesar de esto, es necesario un enfoque más específico en los planes nacionales de ciberseguridad y ciberdefensa como se argumenta a continuación [5].

Los 13 sectores que se mencionan en el párrafo anterior se han desarrollado como objetivos de los diferentes CONPES que hablan de ciberseguridad y ciberdefensa en el país, uno de estos objetivos fue (i) la identificación y caracterización de 13 infraestructuras críticas cibernéticas (ICC), es así como se indican los 13 sectores de ICC del país divididos por impacto así:

- Cuatro sectores que tienen un impacto muy alto en la escala de valoración:
    - Electricidad,
    - Hidrocarburos, minería y gas
    - Financiero
    - TIC;
- Cuatro sectores con impacto alto:
    - Gobierno,
    - Seguridad y defensa,
    - Agua y
    - Transporte;
- Un sector con impacto medio:
    - Industria, comercio y turismo;
- Dos sectores con impacto moderado:
    - Educación y
    - Salud y protección social y, finalmente,
- Dos sectores con un impacto bajo:
    - Ambiente y
    - Agricultura-alimentación.

9.3.4.1 Centro Cibernético de la Policía Nacional (6), (7)

Descripción: Es un centro especializado de atención y respuesta a los delitos que se presentan en el ciberespacio, este centro está formado por un número superior a las 300 personas.

Según indica el ST. Oscar Ivan Mendoza tienen una serie de capacidades cibernéticas y tecnológicas, orientadas a combatir todas las conductas delictivas informadas u observadas por los ciudadanos que hacen uso del ciberespacio llámense personas o empresas públicas o privadas en Colombia.

Este centro está respaldado por una política pública de seguridad digital la cual está contemplada en el CONPES 3701 DE 2011 y en el CONPES 3854 del 2016.

Funciones: El centro cibernético policial cuenta con varios grupos especializados de atención según el delito, ellos son:

- Grupo investigativo de delitos contra la pornografía infantil y otros abusos de internet.

  la ST Katherine Arias indica las tres modalidades atendidas por este grupo:

  - **Sexting:** Intercambio de fotografías eróticas
  - **Grooming:** Una persona suplanta a un niño para comunicarse con otros niños
  - **Sextorsion:** extorsión generada por las fotos intercambiadas.
- Grupo investigativo contra el ciberterrorismo.

  Su misión es descubrir lo de la darknet y realizar una investigación, para combatir el terrorismo que atenta contra los bienes patrimoniales del estado o de privados. El ST. Óscar Iván Mendoza manifiesta que la Policía Nacional de Colombia es un referente en la región, pues cuenta con un oficial de policía en La Haya (Holanda), en Europol. Además, nuestro país es el único de Latinoamérica que tiene una silla en el Centro

Europeo contra el Cibercrimen y esto les permite coordinar operaciones conjuntas, generar intercambio preventivo de información y articularse constantemente con agencias como Ameripol, Interpol y Europol.

- Grupo investigativo de delitos contra la información y los datos.

  Su misión es investigar delitos que atentan contra la información, y los datos de los ciudadanos que son víctimas de suplantación o robos. También investiga delitos cometidos en el sector bancario, la industria y el sector educativo.

- Laboratorio de informática forense.

  Su misión es realizar análisis forenses con herramientas, software especializado y técnicas específicas a equipos móviles celulares, computadoras portátiles, USBs o equipos de networking para extraer evidencia digital, custodiar la información para usarla como prueba válida con los jueces de la república.

Web oficial: https://caivirtual.policia.gov.co/

Logo Oficial:

Figura 8. Logo Centro Cibernético Policial

Redes sociales:

- Twitter: @CaiVirtual Cuenta oficial del Centro Cibernético Policial de la Dirección de Investigación Criminal e INTERPOL
- Facebook: https://www.facebook.com/people/CAI-Virtual-DIJIN/100082118472085/?__tn__=-UC*F
- Instagram: https://www.instagram.com/caivirtual_dijin/?igshid=YmMyMTA2M2Y%3D

- YouTube: https://www.youtube.com/@policiadecolombia/videos

  Fuentes: Diríjase para ver más información a la ruta: Así trabaja el Centro Cibernético Policial | A Colombia la hacemos todos

  Alertas y tips | Equipo de Respuesta a Incidentes de Seguridad Informática de la Policía Nacional CSIRT-PONAL

9.3.4.2 CSIRT Ponal (8)

Descripción: Es el Equipo de respuesta a incidentes de seguridad informática de la policía nacional de Colombia. creado para atender las necesidades de prevención, atención e investigación de los eventos e incidentes de seguridad informática, con el fin de proteger la infraestructura tecnológica, activos de información y mitigar el impacto ocasionado.

CSIRT es un acrónimo y su significado es (Computer Security Incident Response Team)

Objetivos:

- Fortalecer las capacidades institucionales para la prevención, investigación, y atención de eventos e incidentes de seguridad, que atenten contra la confidencialidad, disponibilidad e integridad de la información.
- Proveer asistencia técnica, asesoría y apoyo a la comunidad y a las organizaciones en general, en la protección de amenazas y/o incidentes informáticos. Consolidar los procesos y procedimientos de atención de incidentes de seguridad de la información mediante el uso de estándares y buenas prácticas. Activar los mecanismos de colaboración para la coordinación y gestión de incidentes entre entidades.
- Establecer alianzas estratégicas con organismos nacionales e internacionales, entidades públicas y privadas, para afianzar los mecanismos de ayuda mutua en

materia de seguridad de la información. Fomentar la concienciación en el manejo de la información y la implementación de las políticas de seguridad de la información.

- Generar estrategias de divulgación para suministrar un sistema de alertas tempranas, anuncios y comunicados que permitan prevenir los riesgos asociados a la seguridad de la información. Promover en las organizaciones públicas y privadas la creación e integración de esquemas de atención de incidentes de seguridad CSIRT.
- **Funciones:** El CSIRT-PONAL en su sitio web tiene algunos servicios gratuitos como:
- Análisis de archivos y URLs sospechosas facilitando la rápida detección de virus, gusanos y/o troyanos.
- APK para analista de aplicaciones móviles y
- CTF (Capture The Flag) captura la bandera que corresponde a un juego de seguridad informática ampliamente utilizado por los hackers éticos.

Web Oficial: https://cc-csirt.policia.gov.co/Sandbox

Logo oficial:

Figura 9. Logo CSIRT PONAL Colombia (Computer Security Incident Response Team)

Redes sociales:

- Twitter: @CSIRTPONAL

Fuentes: Diríjase para ver más información a la ruta:

Alertas y tips | Equipo de Respuesta a Incidentes de Seguridad Informática de la Policía Nacional CSIRT-PONAL

9.3.4.3 CCoCi Comando Conjunto Cibernético

Descripción: El Comando Conjunto Cibernético se desempeña como unidad élite en aspectos relacionados con la Ciberseguridad y Ciberdefensa, incluida la protección de las Infraestructuras Críticas Cibernéticas Nacionales, desarrollando operaciones militares en el ciberespacio para defender la soberanía, la independencia, la integridad territorial y el orden constitucional, contribuyendo a generar un ambiente de paz, seguridad y defensa nacional.

Objetivos:

- Las Fuerzas Militares conducen operaciones militares orientadas a defender la soberanía, la independencia, la integridad territorial y derrota de la amenaza, para contribuir a generar un ambiente de paz, seguridad y desarrollo garantizando el orden constitucional de la nación.
- responsabilidad de El Comando Conjunto Cibernético planea, coordina, integra y conduce operaciones militares en el ciberespacio para la defensa de los intereses nacionales y de la infraestructura crítica cibernética nacional a fin de contribuir en el cumplimiento de la misión del Comando General de las Fuerzas Militares

Web Oficial: https://www.ccoci.mil.co/

Logo Oficial:

Figura 10. Logo CCCoCi Comando Conjunto Cibernético Colombia

9.3.4.4 Colcert

Descripción: es el grupo de respuestas a emergencias cibernéticas de Colombia. la misión de ellos es identificar infraestructuras críticas, gestionar sus riesgos de ciberseguridad, ofrecer a las empresas del sector público y privado información preventiva sobre amenazas y vulnerabilidades, apoyo y asesoría en la gestión de los incidentes de ciberseguridad, que garanticen la continuidad de las operaciones y servicios a la ciudadanía colombiana.

Los objetivos del Colcert son:

- Coordinar con las instancias responsables de la Seguridad Digital, entre otros: el Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT), y Sectoriales públicos y/o privados, la compartición de información, para la gestión de amenazas e incidentes de Seguridad Digital Nacional.
- Actuar como punto único de contacto y coordinación para responder de manera rápida y eficiente a incidentes y vulnerabilidades de Seguridad Digital que atenten o comprometan la Seguridad Digital Nacional.
- Coordinar la respuesta a incidentes de Seguridad Digital en las entidades que conforman la Administración Pública en Colombia, en los términos del artículo 39 de la

Ley 489 de 1998 y las normas que modifiquen o sustituyan, y a los particulares que cumplen funciones administrativas.

- Acompañar y apoyar a las entidades que conforman la Administración Pública en Colombia, con el fin de mejorar los procesos de seguridad de la infraestructura tecnológica y la gestión de los incidentes de Seguridad Digital.
- Promover el desarrollo de capacidades locales y sectoriales, así como, la creación de Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT) sectoriales para la gestión operativa de los incidentes de Seguridad Digital en el sector privado y la sociedad civil.
- Desarrollar y divulgar procedimientos, protocolos, guías y recomendaciones de Seguridad Digital para la gestión de incidentes de Seguridad Digital y hacer seguimiento por su implementación y difusión.
- Coordinar la actividad de identificación de las infraestructuras críticas, sujetas a riesgos de seguridad digital, y generar mecanismos de defensa y de protección, en cumplimiento del marco funcional, regulatorio y de responsabilidades en la materia, de conformidad con las libertades y derechos individuales, conforme a la ley vigente.
- Promover la consolidación de espacios de cooperación nacional e internacional para la transferencia de conocimientos y tecnologías, así como la difusión de los conceptos y avances que se producen a nivel nacional e internacional en los temas relacionados con la gestión de amenazas y respuesta a incidentes de Seguridad Digital.
- Mantener actualizado el Sistema de Gestión en cuanto a métodos, controles, procedimientos, manuales, guías, evidencias, registros digitales, indicadores, para las etapas de planificación, ejecución, medición, control, mitigación de riesgos y mejoramiento de los procesos a su cargo.

- Llevar a cabo las actividades necesarias para la atención eficaz y eficiente de los requerimientos de la ciudadanía y los entes de control, formulados por cualquier canal, así como mantener la documentación a su cargo de acuerdo con los lineamientos y procedimientos establecidos por el Ministerio.
- Dar cumplimiento a los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI), asociados a la protección de la información.
- Adelantar las actividades encaminadas al mejoramiento continuo de los asuntos de su competencia, en el marco de la implementación y sostenibilidad del Modelo Integrado de Planeación y Gestión (MiPG), y frente a los hallazgos derivados de las auditorías internas y externas.

Figura 11. Modelo relacional del ColCERT. fuente ministerio de defensa

web Oficial: https://www.colcert.gov.co/

Logo Oficial:

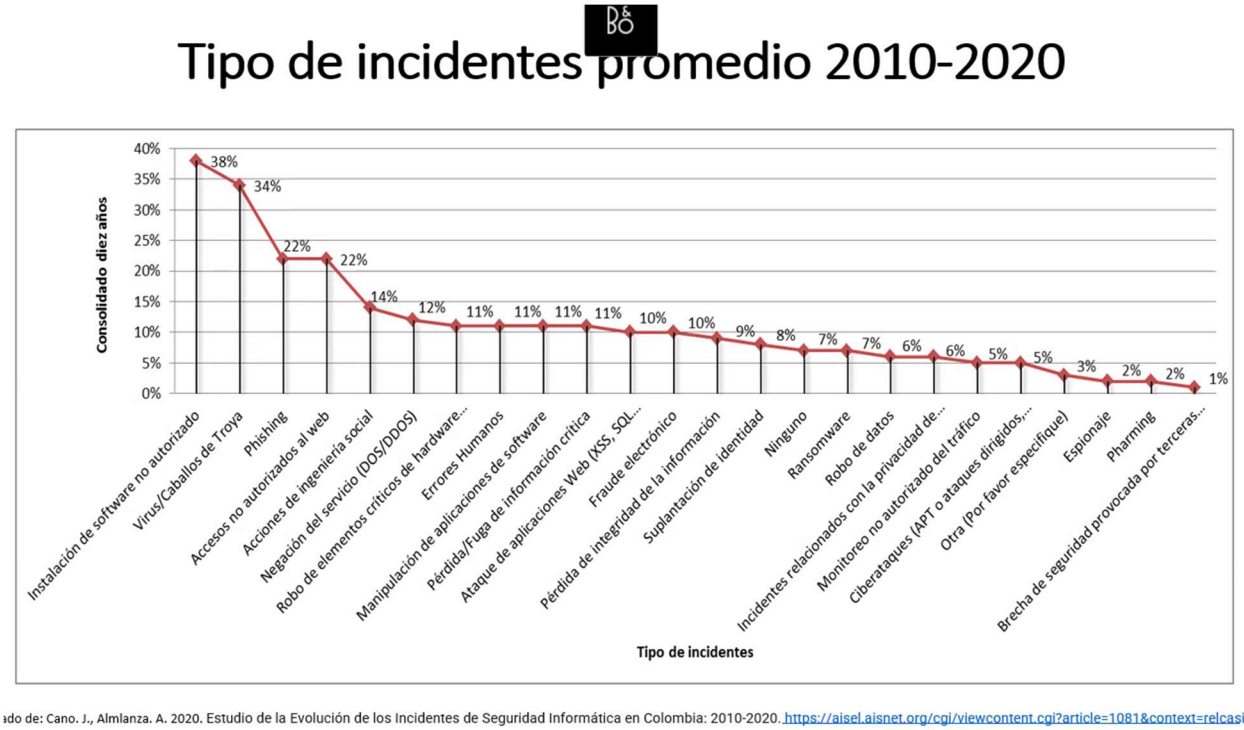
Figura 12. Logo de ColCERT Grupo de Respuesta a Emergencias Cibernéticas Colombia

Redes sociales: Twitter:

Paginas de interes en la web @ColCERT

- https://www.colcert.gov.co/800/w3-propertyvalue-412601.html BOLETINES DE INFORMACIÓN:

9.3.5 Estadísticas



ıdo de: Cano. J., Almlanza. A. 2020. Estudio de la Evolución de los Incidentes de Seguridad Informática en Colombia: 2010-2020. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1081&context=relcasi

Figura 13. Tipos de incidente

9.3.5.1 Estadísticas del Centro Cibernético de la Policía Nacional

Según datos entregados por la entidad “entre enero y octubre de 2022 en Colombia la cifra de ataques se multiplicó a 54121 denuncias” (9). Y fueron más de 30 las empresas que sufrieron la situación (9) de afectación por ransomware, en el año 2021 el número fue de 11.223 casos registrados (10).

9.3.5.2 Estadísticas de la Región

Fortinet ha señalado que Colombia está entre el top de los países de Latinoamérica con más intentos de ciberataques. en ese orden se destaca en primer lugar, México con 85 millones, seguido de Brasil Con 31.500 millones y Colombia con 6300 millones de intentos de ataques, los cuales han sigo con estrategias más sofisticadas y dirigidas como es el caso del ransomware (secuestro de información). Ahora durante los primeros seis meses de 2022 se detectaron cerca de 384000 millones de intentos de distribución de ransomware en todo el mundo, de estos 52.000 millones iban dirigidos a Latinoamérica. informó **Fortinet** (10).

IBM a través de Diana robles experta en temas de ciberseguridad para la región dejó saber algunos datos estadísticos lo cuáles son datos de un estudio de IBM así, el phishing es la causa más común de ciberataques (47%) en 2021, el estudio también arrojó un dato que indicó un aumento de los ataques provocados por credenciales robadas o ransomware del 29% en américa latina.

9.2.5.3 Estadísticas del Mundo.

Obrela Security Industries en un estudio realizado para el Reino Unido indica que más de las cuatro quintas partes de las organizaciones de atención médica del país antes mencionado sufrieron un ataque en el último año (2021) (11).

ITU indica que la ciberseguridad tiene un amplio campo de aplicación, que abarca muchas industrias y varios sectores, el nivel de desarrollo o compromiso de cada país se evalúa en cinco pilares: Medidas legales, Medidas técnicas, Medidas organizativas, Desarrollo de capacidades, y Cooperación", dice el Índice de Ciberseguridad Global (GCI) Int'l Telecommunication Union, y su publicación sobre Índice de Ciberseguridad Global (GCI).

De acuerdo con el estudio, Colombia alcanzó un puntaje de 63.72, divididos de la siguiente manera: medidas legales 9.14, medidas técnicas 17.58, medidas organizativas con 6.67, capacidad de desarrollo 14.42 y medidas cooperativas con 15.93 unidades (12).

9.3.6 Empresas del Sector Salud Atacadas en Colombia

En Colombia se han reportado oficialmente ciberataques a empresas del sector salud como:

- **Audifarma:** atacada el 22 de enero de 2023 deshabilitó preventivamente sus sitios web www.audifarma.com.co Audifarma app, turno digital, solicitud de medicamentos.
- **Keralty EPS Sanitas, Medicina prepagada Colsanitas**, Atacada en noviembre de 2022 De acuerdo con Juan Pablo Rueda, presidente de la EPS Sanitas, la entidad fue víctima de un ataque cibernético que llevó a la empresa a desarrollar un *"plan de contingencia"*, manifestó. Adicionalmente, desde Sanitas se confirmó que la Fiscalía General de la Nación abrió una investigación para confirmar quiénes estarían detrás del ataque (10).

- Sobre Keralty: es un proveedor de atención médica que opera una red internacional de 12 hospitales y 371 centros médicos en América Latina, España, Estados Unidos y Asia, emplea a 24.000 personas y tiene 10.000 médicos que brindan atención médica a más de 6 millones de pacientes (13)
- Sobre el ataque sufrido por Keralty algunos usuarios reportaron imágenes del evento que se indican a continuación: La imagen siguiente es un recorte de un

usuario de twitter @ElChrissoy

Figura 14. Portal de EPS Sanitas atacado por un ransomware. Nov 2022

- Famisanar
- Invima

9.3.7 Efectos de los Ataques

Algunos de los problemas evidenciados luego de un ataque cibernético a infraestructura crítica de servicios de salud son la afectación de servicios como:

- Entrega de medicamentos
    - en ventanilla
    - a domicilio
- Agendamiento de citas
- Agendamiento de cirugías
- Pérdidas de productividad
- Pérdidas de ingresos
- Parálisis o interrupción operativa
- Incumplimientos contractuales
- Pérdida de información sensible de clientes o usuarios

9.3.8 Tipos de Empresas Atacadas

Compañías públicas y privadas de gran prestigio, en teoría preparadas, no han escapado de ser víctimas

"Todos los años se baten récords en las estadísticas sobre el número de ataques y pérdidas económicas generadas por el ransomware, con efectos que pueden ser verdaderamente catastróficos y, en consecuencia, probablemente puedan llevar al extremo de poner en riesgo la supervivencia de las organizaciones", explica German Vargas Pedroza, oficial de Riesgos Corporativos de Claro Colombia

9.3.8.1 Que Áreas de las Empresas son más Vulnerables?

Los expertos indican que las modalidades son cada vez más sofisticadas, lo que hace que cualquier área de la empresa sea vulnerable y sensible a los ataques.

Diana Robles, líder de IBM Security para Colombia, Perú, Ecuador, Venezuela y Región Caribe, explicó que cualquier área o *información crítica* de una empresa es susceptible a la hora de enfrentarse a un ciberataque. La diferencia la hacen las empresas que están preparadas para contener y detectar rápidamente un ciberataque y de esta manera contener la fuga y la propagación del ataque (10).

Kelly quintero líder de Beyond trust indica sobre el tema que “los controles de seguridad informática nunca serán suficientes para cuando estar preparados ante ataques cibernéticos se refiere” (10)

9.3.9 Colectivos de Ciberatacantes

Los colectivos de ciberatacantes:

9.3.9.1 Lapsus$ (14):

Se ha convertido en el grupo de ciberdelincuentes más temido por las empresas durante este 2022 y no es para menos, ya que, en tan solo unas semanas, ha conseguido acceder a datos confidenciales de grandes empresas tecnológicas como Microsoft, Samsung o Nvidia Ubisoft.

Algo que caracteriza a Lapsus$ es que anuncian sus ataques en redes sociales e incluso comentan lo que pretenden con sus ciberataques. Tienen un canal de Telegram en el que realizan encuestas con los usuarios para escoger sus próximos objetivos y en el que cuentan con miles de seguidores.

Asimismo, varias investigaciones afirman que detrás de este grupo hay jóvenes hackers de entre 16 y 21 años.

9.3.9.2 REvil (14):

Durante 2020 y 2021 REvil era una de las bandas de ciberdelincuentes más populares, hasta que, a principios de 2022, fuera desmantelada por el FBI.

Utilizaban el ransomware, un ataque *hacker* que encripta todos los datos de los discos duros de las víctimas y que solo se pueden desencriptar con una clave que los delincuentes venden a las víctimas a precio de oro. Cobrando dinero por las claves de desencriptado, REvil habría recaudado decenas de millones de euros.

Uno de sus mayores ataques fue a Colonial Pipeline, el sistema de oleoductos más grande para productos de petróleo refinado en Estados Unidos. El *hackeo* obligó a parar sus operaciones durante días, lo que supuso un inconveniente para los suministros de carburantes en el país norteamericano.

Supuestamente, REvil también estuvo detrás del *hackeo* a un proveedor de Apple, que reveló el diseño de los MacBook Pro, antes de que se realizará el lanzamiento oficial.

9.3.9.3 RansomHouse (15):

En su sitio web de la Dark Web se autodenominan como una comunidad de mediadores profesionales que “no utilizan ni producen ningún ransomware, su principal objetivo es minimizar los daños que puedan sufrir las partes relacionadas. Conduciendo a acuerdos amistosos y a veces incluso de manera posterior a cooperación productiva y amistosa.”

Para esta comunidad la culpa de los ciberataques “no son los que encontraron la vulnerabilidad o llevaron a cabo el hackeo”, sino los responsables de ciberseguridad se las

empresas “que no pusieron un candado en la puerta y la dejaron abierta, invitando a entrar a todo el mundo”.

Según BleepingComputer, se cree que RansomHouse inició su actividad en diciembre de 2021. La primera mención de este grupo se produjo con la publicación de un ransomware llamado White Rabbit.

9.3.9.4 ViceSociety:

ViceSociety es un grupo de piratería conocido por los ataques de extorsión de ransomware en organizaciones educativas y de atención médica. Se cree que son de habla rusa. Han atacado objetivos tanto en Europa como en los Estados Unidos, incluido un compromiso importante del Distrito Escolar Unificado de Los Ángeles.

9.3.9.5 BlackCat o ALPHV:

Descripción: Es un grupo reconocido por la criptografía aplicada, la cual no permite atacar el algoritmo utilizado actualmente y será necesario contar con las llaves de los atacantes en caso de querer recuperar la información secuestrada

Pysa:

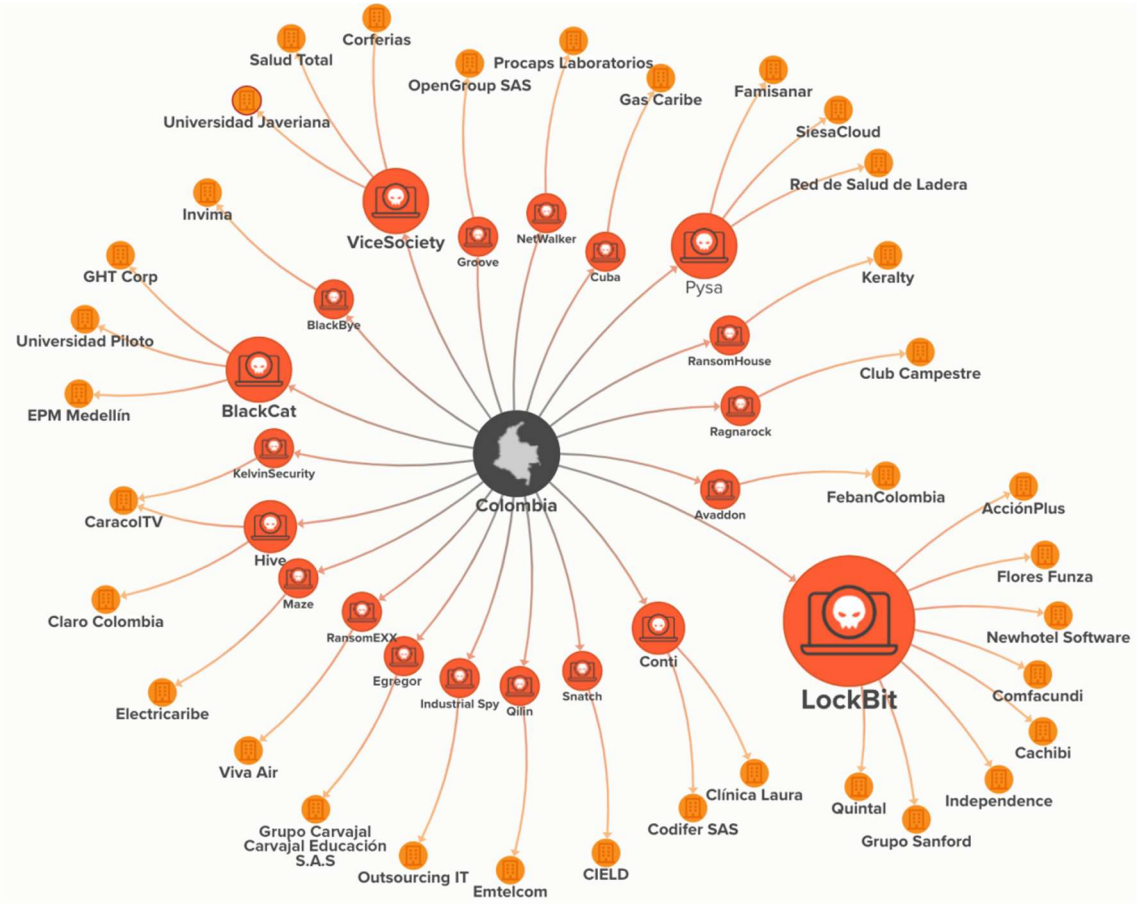


Figura 15. Entidades colombianas atacadas por grupos de ransomware(16)

9.3.9.6 Ciclo del Ransomware

Se presenta el ciclo de vida de un incidente de ransomware

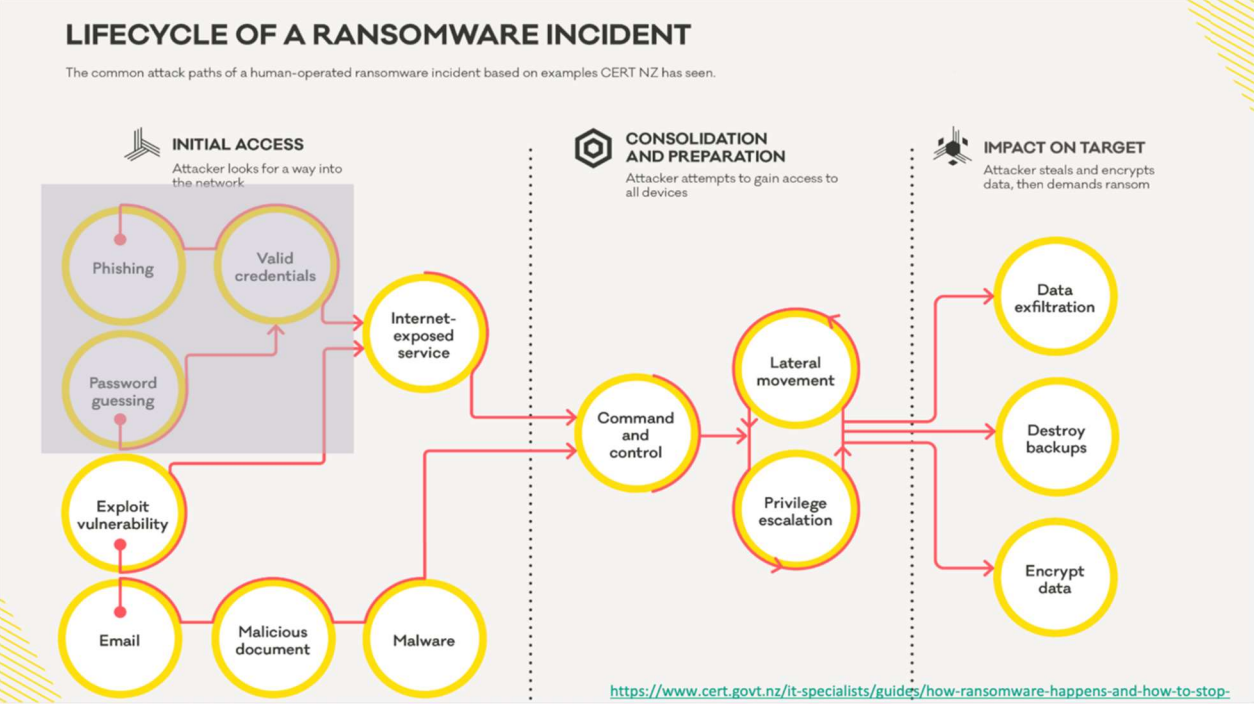


Figura 16. Ciclo de vida del ransomware (17)

9.3.10 Tipos de Ciberatacantes (18)

Se pueden perfilar a los ciberdelincuentes que existen y a cada uno de ellos atribuirle ciertas características, de igual manera las personas que optan por este oficio no necesariamente están dedicadas al robo informático o a la amenaza o a generar daño tanto a personas como gobiernos. Este perfilamiento se da de acuerdo con sus intenciones.

Una definición de la RAE de un hacker es: Hacker o Pirata Informático es una persona con grandes habilidades en el manejo de computadoras que investiga un sistema informático para avisar de los fallos y desarrollar técnicas de mejora.

Persona con amplios conocimientos en tecnología, informática, electrónica y comunicaciones que siempre está con el estado del arte de las herramientas informáticas y conoce detalladamente la programación y sistemas complejos.

A continuación, se indican los tipos así:

9.3.10.1 BlackHat Hackers

Descripción: Hackers de Sombrero Negro son los chicos malos o los ciberdelincuentes, los que comúnmente se les refiere como Hackers. El término se usa específicamente para los Hackers que rompen la seguridad de una computadora o una red de datos sin consentimiento con el fin de infringir daños, obtener información financiera, datos personales, contraseñas o crean virus de computadora para introducirlos. Estos muestran sus habilidades en informática rompiendo sistemas de seguridad, colapsando servidores, entrando a zonas restringidas, infectando redes o apoderándose de ellas, utilizando sus destrezas en métodos hacking.

9.3.10.1.1 Crackers

Descripción: Estos comúnmente entran en sistemas vulnerables y hacen daño robando información, modificando o borrando información, dejando algún virus, malware o troyano en el sistema o creando y dejando puertas traseras para poder entrar nuevamente cuando les plazca.

9.3.10.1.2 Phreaker

Descripción: Es aquella persona que con amplios conocimientos de telefonía puede llegar a realizar actividades no autorizadas con los teléfonos, por lo general celulares. Construyen equipos electrónicos artesanales que pueden interceptar y hasta ejecutar llamadas de aparatos telefónicos celulares sin que el titular se percate de ello. En Internet se distribuyen

planos con las instrucciones y nomenclaturas de los componentes para construir diversos modelos de estos aparatos.

9.3.10.2 WhiteHat Hackers

Descripción: Hackers de Sombrero Blanco son los chicos buenos, o **Hackers éticos**. Regularmente son los que penetran la seguridad de sistemas para encontrar vulnerabilidades, se centran en asegurar y proteger los sistemas TI, Tecnologías de información y comunicación. Algunos son consultores de seguridad, trabajan para alguna compañía en el área de seguridad informática protegiendo los sistemas de los BlackHat Hackers.

9.3.10.3 GrayHat Hackers

Descripción: Hackers de Sombrero Gris son los que juegan a ser los buenos y los malos, en otras palabras, tienen ética ambigua dependiendo del momento y del lugar, prestan sus servicios a agencias de inteligencia, grandes empresas o gobiernos.

Por lo general no hackean para beneficio personal ni tienen intenciones maliciosas, pero pueden estar dispuestos a realizar intrusiones a sistemas con fines ambiguos usando su conocimiento por ejemplo para informar e incrementar la seguridad de la red vulnerada o para afectar críticamente servicios e infraestructura.

9.3.10.4 RedHat Hackers

Descripción: Hacker que dentro de sus objetivos está en detener de una manera agresiva a los BlackHat Hackers, y de manera general a los hackers que realizan malas acciones en la red.

9.3.10.5 BlueHat Hackers

Descripción: Hacker que utiliza técnicas para ganar popularidad entre sus pares y ajustar cuentas con sus adversarios. Estos realizan hackeos peligrosos debido a las intenciones maliciosas y están más allá que la intención de querer aprender.

9.3.10.6 Purple Hat Hackers

Descripción: Hacker que tiene dos definiciones populares definiéndolo como persona que realiza el hacking sobre sus propios sistemas. También se encuentra que el púrpura es la mezcla del color rojo y el azul entonces lo purple hat hackers son frecuentemente vistos como el puente que conecta los pentester y los defenders, esta combinación da un hacker que protege y ataca el ambiente en el que se desenvuelve.

9.3.10.7 GreenHat Hackers o Newbie

Descripción: Hacker Novato el que se tropieza con una página web sobre Hacking y baja todas las utilidades y programas a su PC, comienza a leer y ejecutar los programas para ver qué hacen.

Se refiere a un recién iniciado en la informática. Y hace referencia a las personas realmente interesadas en aprender, y que no buscan que los demás integrantes de la comunidad o foro a la que pertenecen solucionen sus problemas. También se usan abreviaciones como "Noob" o "Newb" que son bastante usadas como insulto, aunque no lo son.

9.3.10.8 Script Kiddies

Descripción: Hackers que utilizan programas escritos de otros para penetrar algún sistema, red de computadora, página web o base de datos, ya que tiene poco conocimiento sobre lo que está pasando internamente en la programación. Es habitual asumir que los scripts

kiddies son personas sin habilidad para programar sus propios medios, y que su objetivo es intentar impresionar a sus amigos o ganar reputación.

9.3.10.9 Hacktivistas

Descripción: Hackers que utilizan sus habilidades para atacar una red con fines políticos, como lo hace Anonymous.

9.3.10.10 Whistleblower

Descripción: más que un hacker es un informante malicioso. Este término se usa mucho a nivel corporativo y se refiere a personas que no están contentas con su trabajo o que han sido contratadas por la competencia para infiltrarse y revelar secretos de la competencia.

9.3.10.11 Lammer

Descripción: Es aquella persona que se cree Hacker y no tiene los conocimientos necesarios ni la lógica para comprender qué es lo que realmente está sucediendo cuando utiliza algún programa ya hecho para hackear y romper alguna seguridad. Muchas veces se hace pasar por un Hacker.

Es el que ha bajado cientos de libros y videos de sitios donde se propaga la piratería de diversos temas de hacking, te lo dice y no ha leído ni visto ninguno de los videos, solamente los almacena. Se trata de una persona que presume de tener unos conocimientos o habilidades que realmente no posee y que no tiene intención de aprender.

Figura 17. Tipos de hacker.

9.3.11 Tipos de Ataques

9.3.11.1 Ransomware

Descripción: Software Malicioso (Malware) que infecta los dispositivos y cifra los archivos del sistema toma el control y secuestra la información, su propósito es la obtención de un rescate a través de bitcoins a cambio de eliminar la restricción (19)

Características:

- Uso de software legítimo para acceder a las organizaciones y tomar control del mayor número de sistemas a su alcance.
- Configura archivos de encriptación para múltiples sistemas operativos que permiten generar un mayor impacto a las organizaciones afectadas.
- Incluyen una herramienta identificada como ExMatter, la cual ha sido desarrollada para extraer información usando mecanismos de división de grandes volúmenes de datos en piezas más pequeñas, que tratan de simular tráfico de navegación y pueden evadir los controles de monitoreo

Métodos de Propagación: Entre algunas de las formas en que estos programas informáticos se propagan, están:

- Usan correos con enlaces para infectar sistemas, que alguien en la organización afectada abre engañosamente.
- Al visitar sitios web de dudosa reputación.
- Al conectar dispositivos USB infectados con este software

Recomendaciones:

- Evite dar clic sobre links o archivos adjuntos en correos electrónicos desconocidos.
- Realice copias de seguridad de datos con regularidad y protéjase con contraseña.

- Cree un air gap (desconectar los dispositivos de la red), ya que es una forma efectiva de preservar los datos de los daños ante un ataque Ransomware.
- Requiere credenciales de administrador para instalar el software.
- Evite ingresar a sitios web de dudosa reputación o contenido censurado.
- Verifique los correos, ejecutando los enlaces o archivos en un entorno sandbox.
- Utilice la autenticación multifactor cuando sea posible.
- REPORTE cualquier incidente.

Datos técnicos: En América Latina, las cinco familias más comunes de ransomware son Trojan.Ransom, Win 32.Wanna, Trojan.Ransom.Win32.Stop, Trojan.Ransom.Win 32.Blocker, Trojan.Ransom.MSIL.Blocker y VHO.Trojan.Ransom.Win 32.Convagent, todos ellos encryptors, es decir que, como su nombre lo dice, encriptan los datos de sus víctimas.(19)

Se reportan ransomware de la región y uno de ellos se llama el chile locker, fue diseñada por cibercriminales latinoamericanos con la capacidad de robar credenciales guardadas en navegadores, enumerar dispositivos de extracción (como discos duros y pendrives) para el cifrado y evadir la detección por antivirus mediante tiempos de espera de ejecución. Hasta la fecha, Chile Locker solo se ha detectado en la región (19)

Grupo de ciberdelincuentes: RansomHouse

9.3.11.2 Pishing (20)

Descripción: En este ataque, mensajes que parecen legítimos manipulan a un usuario, haciéndole instalar un archivo malicioso, hacer clic en un enlace malicioso o divulgar información sensible como credenciales de acceso.

Características:

- El correo falso

Métodos de Propagación: mensajes de texto, correos electrónicos

Recomendaciones:

- No abra el enlace y evite dar clic, sobre links o archivos adjuntos en correos electrónicos desconocidos.
- Tenga en cuenta, que ningún banco solicitará información y/o actualización de productos por correos electrónicos.
- Verifique ortografía y redacción, usualmente hay errores.
- Verifique que el dominio del correo del remitente corresponda a la entidad bancaria.
- No ingrese ningún tipo de información en el formulario mostrado en este sitio web.
- Reporte el enlace con el CAI Virtual a través de la web: https://caivirtual.policia.gov.co
- En caso de ser víctima reporte al banco dicho incidente para que realicen las diligencias de acuerdo a su competencia.
    - En caso de ser víctima cambie de inmediato la clave de su cuenta**.**

9.3.11.3 Spear- Pishing

Descripción: Técnica de Ingeniería social. Mediante esta modalidad la víctima entrega datos personales y financieros en sitios web bancarios aparentemente oficiales.

Estos datos están siendo usados para transferencias no consentidas de activos, suplantación y accesos abusivos a sistemas informáticos. Ataque dirigido a un objetivo específico (21).

En resumen, es el engaño a la víctima, haciéndose pasar por una marca o persona para que entregue datos.

Características:

- El correo falso de la entidad bancaria suplantada, le indica a la víctima que para validar la información, debe dar clic en el botón titulado “Ingresar”, que redirecciona a la potencial víctima al link: http://bitly.ws/yUdT

  Métodos de Propagación: mensajes de texto, correos electrónicos

Recomendaciones:

- Evite dar clic sobre links o archivos adjuntos en correos electrónicos desconocidos. No
- Ingrese ningún tipo de información en el formulario mostrado en este sitio web.
- Reporte el enlace con el CAI Virtual a través de la página web: https://caivirtual.policia.gov.co
- En caso de ser Víctima. Reporte al banco dicho incidente para que realicen las diligencias de acuerdo a su competencia.
- En caso de ser Víctima. Cambie de inmediato la clave de su cuenta donde relacionen información de su entidad bancaria.

9.3.12 Tácticas Para Evitar Mitigar Ataques

Por lo general, suspender servicios internos de la organización, eliminar el acceso del administrador a los sistemas y respaldar la información sensible, eliminar el uso de contraseñas y establecer políticas de cambio frecuente de las mismas.

Por último, realizar una constante evaluación de las vulnerabilidades de software, aplicaciones y otros sistemas. (10)

10. Metodología

La metodología implementada para diseñar la arquitectura de ciberseguridad para la IPS Calculaser S.A está basada en las normas ISO 27001:2013 y la ISO 27005:2011 y las experiencias vividas en el ámbito tecnológico por cada uno de los participantes en la construcción de este proyecto de grado; así mismo se encuentra alineada con los objetivos estratégicos de la organización.

10.1 Línea de investigación

Tomando como referencia las normas ISO/IEC 27001:2013, ISO 27005:2011, ISO 27032:2012, se puede determinar que la línea de investigación del presente trabajo está relacionada con los siguientes temas:

- Seguridad de la información
- Gestión de Riesgos
- Ciberseguridad

Este trabajo se aplicó en la organización Calculaser S.A., ubicada en la zona denominada eje cafetero, Colombia, donde existen 5 sedes interconectadas a través de la internet.

10.2 Instrumento de Recolección de Información

Para el desarrollo del siguiente trabajo de grado, se utilizaron los siguientes mecanismos e instrumentos para la recolección de la información:

- Observaciones
- Entrevistas con funcionarios líderes de proceso y con usuarios responsables de los activos de información y sobre todo con el personal de apoyo en el área de TI.
- Documentación existente del sistema de gestión de calidad.
- Evaluaciones con experiencias de los autores del presente documento.

Además, se usaron diferentes fuentes de información, tales como tesis, artículos, normas y búsquedas en internet.

10.3 Fases Metodológicas

Teniendo en cuenta los requerimientos establecidos en las normas de la línea de investigación de acuerdo con las buenas prácticas de las mismas se establecieron las siguientes fases para el desarrollo del proyecto:

10.3.1 Inventario de activos de información

Se elaboró un inventario y una clasificación de activos de información que incluyó la observación directa en cada una de las sedes físicas y entrevistas con los líderes de proceso y usuarios responsables de los activos de información.

10.3.2 Gestión de Riesgos

La gestión de riesgo de la organización fue basada en la norma ISO 27005:2011, según los numerales 7: establecimiento del contexto, 8: evaluación de los riesgo, 9: tratamiento de los riesgos y 10: aceptación de los riesgos; además de seguir el proceso de la misma, como lo ilustra la siguiente figura:

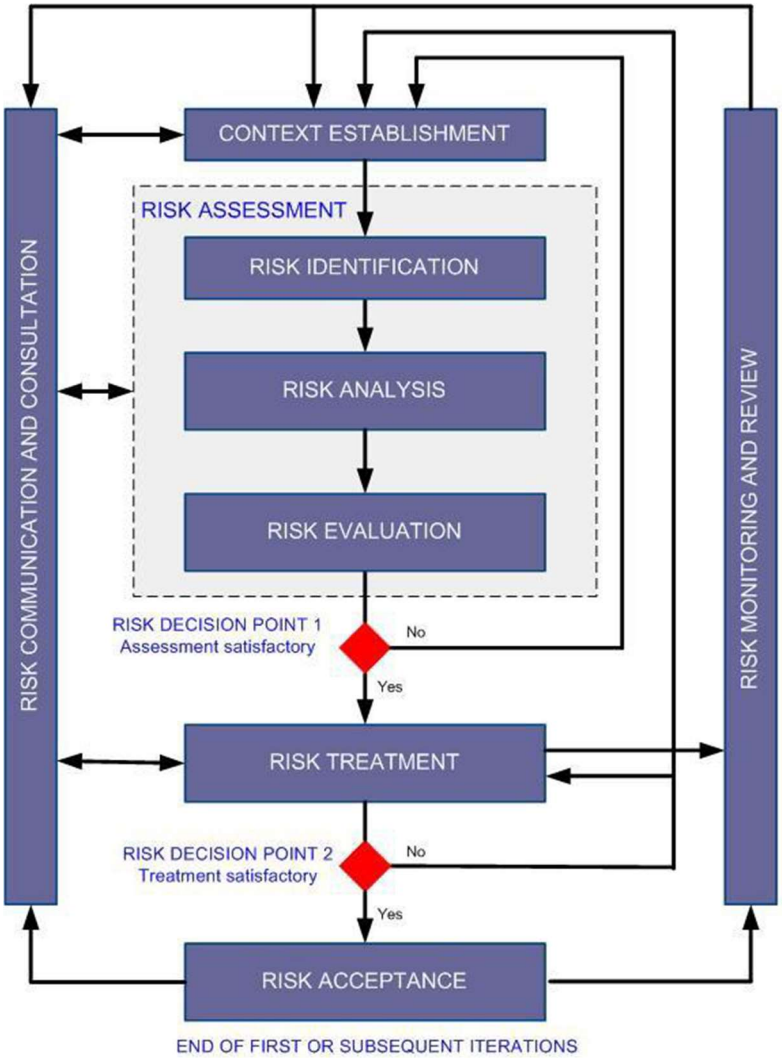


Figura 18. Proceso de gestión de riesgos según ISO-IEC 27005:2011

Nota. Fuente Norma ISO/IEC 27005:2011

NOTA: El plan de continuidad del negocio y plan de respuesta a incidentes, no hacen parte del alcance del presente trabajo de grado.

10.3.3 Definición de Arquitectura de Ciberseguridad

Para lograr este objetivo específico se tomaron como insumo los planes de acción técnicos derivados del proceso de gestión de riesgos y socializados en el plan de tratamiento de riesgos (ver tabla 10), para garantizar y minimizar la materialización de estos. Se tomó como referencia el fabricante Check Point, catalogado como el proveedor de soluciones de ciberseguridad con mejor desempeño en el mercado.

La estrategia de ciberseguridad integral de Check Point se basa en varios pilares:

Firewall de red: Check Point ofrece firewalls de red de alto rendimiento que protegen la red de una organización contra ataques cibernéticos y amenazas avanzadas. El firewall se basa en tecnología de inspección profunda de paquetes (Deep Packet Inspection, DPI) y en la identificación de aplicaciones para ofrecer una mayor seguridad.

Detección y Prevención de intrusiones (IDS/IPS): Esta solución utiliza tecnología de inspección en línea para proteger la red contra ataques de malware, exploits y otras amenazas conocidas y desconocidas.

Seguridad para endpoints: Check Point Endpoint Security ofrece protección para dispositivos de usuarios finales, como portátiles, teléfonos móviles y tablets, mediante el uso de un motor de prevención de amenazas y políticas de seguridad para proteger contra el malware, exploits y otros ataques.

Seguridad en la nube: Check Point CloudGuard protege las aplicaciones y datos en la nube, asegurando que sólo los usuarios autorizados tengan acceso a los recursos de la nube. Además, ofrece protección contra amenazas avanzadas, como los ataques DDoS.

Seguridad e correo electrónico: Check Point Email Security ofrece protección para correo electrónico, como Gmail y Office 365, mediante el uso de un motor de prevención de amenazas y políticas de seguridad para proteger contra el malware, exploits, phishing, BEC y otros ataques.

Gestión centralizada: Check Point ofrece una plataforma centralizada de gestión y control que permite la administración y monitoreo de todos los componentes de seguridad en la red de una organización.

Protección en todas partes: Check Point ofrece una amplia gama de soluciones de seguridad para proteger los sistemas, redes y dispositivos móviles de sus clientes, incluyendo firewalls, sistemas de prevención de intrusiones, soluciones de seguridad de correo electrónico y endpoint protection. Además, Check Point proporciona soluciones de seguridad en la nube para proteger los datos que se encuentran en la nube.

Gestión unificada de políticas: Check Point proporciona una plataforma de gestión de seguridad centralizada que permite a los clientes gestionar todas las políticas de seguridad desde una única consola. Esto permite una mayor eficiencia en la gestión de la seguridad y una mayor visibilidad de las amenazas en toda la organización.

Prevención avanzada de amenazas: Check Point utiliza tecnologías avanzadas de prevención de amenazas, incluyendo inteligencia artificial y aprendizaje automático, para detectar y prevenir amenazas conocidas y desconocidas. También proporciona una amplia

gama de herramientas de análisis de seguridad para ayudar a los clientes a identificar y responder rápidamente a las amenazas.

Colaboración global: Check Point mantiene una estrecha colaboración con agencias de inteligencia y organizaciones de seguridad en todo el mundo para asegurarse de que sus soluciones están actualizadas con las últimas amenazas y tendencias de seguridad.

En resumen, la arquitectura de seguridad de Check Point se basa en un enfoque integrado y completo para la protección de redes, datos y sistemas de una organización, ofreciendo una mayor visibilidad, control y seguridad.

11. Resultados y discusión

11.1 Inventario de Activos de Información

Uno de los controles de la norma ISO 27001:2013, es el inventario de los activos de información (A.8.1.1) que dan soporte a los procesos estratégicos, misionales y de apoyo de Calculaser (Figura 1. - Mapa de procesos), gestionando la identificación y clasificación donde se establece el responsable o propietario de cada activo (A.8.1.2)

Dada la necesidad de saber con qué activos de información cuenta en la actualidad Calculaser S.A., se procede a elaborar el inventario y clasificación teniendo en cuenta que:

- Calculaser S.A. posee información que se debe proteger como son las historias clínicas consideradas como información sensible que se encuentra almacenadas en los sistemas de información ISalud, frente a las amenazas, vulnerabilidades y posibles riesgos que afecten la continuidad del negocio.
- Los activos de información son todos aquellos elementos lógicos o físicos que conforman la infraestructura tecnológica de la organización, clasificados de la siguiente forma:
    - Información,
    - Bases de datos,
    - Servicios,
    - Software (aplicaciones),
    - Hardware (hardware),
    - Comunicaciones,
    - Recursos administrativos,

- Recursos físicos y,
- Recursos humanos.

Para garantizar el cumplimiento del primer objetivo específico, el cual refiere realizar un inventario de activos de información con énfasis en hardware (C-HDW), software (C-SFW) y servicios tecnológicos (C-SRV), se elaboró el inventario con los líderes de proceso y los usuarios responsables de cada activo, además con el acompañamiento del personal de apoyo TI, quienes se encargaron de proporcionar la información detallada y requerida.

En la tabla 3, que se encuentra en la siguiente página, se especifican los datos de los 95 activos de información identificados y clasificados, además el proceso a donde pertenecen, ubicación física, el propietario y el responsable.

Según la norma ISO 27001:2013 un activo es todo aquello que tiene valor para la entidad y que, por lo tanto, requiere de protección.
La identificación de activos se debería llevar acabo con un nivel adecuado de detalle que proporcione información suficiente para la valoración del riesgo. Para realizar esta identificación es necesario revisar la guía de gestión de activos.

Nro	Proceso	Area o Departamento	Tipo de activo (Servicio/C-SRV, Software/C-SFW, Hardware/C-HDW)	Identificador	Nombre del activo	Descripción del activo	Ubicación física	Propietario	Responsable (Custodio)
1	Misionales	Institucional	C-SFW	8080111	HIS / ISalud	Sistema Gestion Medica	Nube	Gerente	Apoyo TI
2	Apoyo	Gestión Contable-Administrativa	C-SFW	8080112	ERP / Yeminus	Sistema Gestion Financiera y Contable	Nube	Contadora	Luisa Holguin
3	Estrategico	Institucional	C-SFW	8080115	Kaspersky	Solucion de Antivirus	Local	Gerente	Apoyo TI
4	Estrategico	Institucional	C-SFW	8080117	Microsoft 365 APP	Herramienta Ofimatica	Local	Gerente	Apoyo TI
5	Misionales	Gestion prestacion de servicios	C-SRV	8080114	Plataforma de Call Center	Plataforma de Call Center	Nube	Directora Prestacion de Servicios	Prestacion de Servicios
6	Estrategico	Institucional	C-SRV	8080116	Correo - Google Workspace	Solucion Correo y Colaboracion	Nube	Gerente	Apoyo TI
7	Apoyo	Gestión de Calidad	C-SRV	8080118	Portal Corporativo	Portal Corporativo	Nube	Coord. Calidad	Ana Marcela Ossa
8	Apoyo	Institucional	C-SFW	8080119	Plexo	Plataforma de Capacitacion	Nube	Coord. Gestion Humana	Lucy Huertas
9	Estrategico	Gestion Gerencial	C-HDW	5202032	Firewall(Asis)	Soporte a reglas de seguridad de la organización, sede	Sede Asistencial	Gerente	Apoyo TI
10	Estrategico	Institucional	C-HDW	5202033	Srv-Zeus	Servidor de archivos	Sede Administrativa	Gerente	Apoyo TI
11	Estrategico	Gestion Gerencial	C-HDW	5202857	Firewall(Adm)	Soporte a reglas de seguridad de la organización, sede	Sede Administrativa	Gerente	Apoyo TI
12	Apoyo	Gestión Humana	C-HDW	5202999	PC	Equipo de Computo	Sede Administrativa	Coord. Gestión Humana	Lucy Huertas
13	Apoyo	Gestión Humana	C-HDW	5202011	PC	Equipo de Computo	Sede Administrativa	Coord. Gestión Humana	Lucy Huertas
14	Apoyo	Gestión Humana	C-HDW	5202031	PC	Equipo de Computo	Sede Administrativa	Coord. Gestión Humana	Lucy Huertas
15	Misionales	Gestion prestacion de servicios	C-HDW	5202007	PC	Equipo de Computo	Sede Administrativa	Directora Prestacion de Servicios	Adriana Martinez
16	Misionales	Gestion prestacion de servicios	C-HDW	5202006	PC	Equipo de Computo	Sede Administrativa	Directora Prestacion de Servicios	Supernumerario
17	Apoyo	Gestión Contable-Administrativa	C-HDW	5202005	PC	Equipo de Computo	Sede Administrativa	Contadora	Tatiana Lopez
18	Misionales	Gestion prestacion de servicios	C-HDW	5202009	PC	Equipo de Computo	Sede Administrativa	Directora Prestacion de Servicios	Lorena Puerta
19	Misionales	Gestion prestacion de servicios	C-HDW	5202008	PC	Equipo de Computo	Sede Administrativa	Directora Prestacion de Servicios	Juan David Echeverry
20	Estrategico	Gestion Gerencial	C-HDW	5202014	PC	Equipo de Computo	Sede Administrativa	Gerente	Cristina Osorio

Tabla 3. Inventario de activos de información.

Fuente. Elaboración propia

Nro	Proceso	Area o Departamento	Tipo de activo (Servicio/C-SRV, Software/C-SFW, Hardware/C-HDW)	Identificador	Nombre del activo	Descripción del activo	Ubicación fisica	Propietario	Responsable (Custodio)
21	Misionales	Gestion prestacion de servicios	C-HDW	5202029	PC	Equipo de Computo	Sede Administrativa	Directora Prestacion de Servicios	Bryan Salas
22	Apoyo	Gestión Humana	C-HDW	5202048	PC	Equipo de Computo	Sede Administrativa	Coord. Gestión Humana	Lucy Huertas
23	Misionales	Gestion prestacion de servicios	C-HDW	5202016	PC	Equipo de Computo	Sede Administrativa	Directora Prestacion de Servicios	Isabela Betancur
24	Apoyo	Gestión Humana	C-HDW	5202018	PC	Equipo de Computo	Sede Administrativa	Coord. Gestión Humana	Lucy Huertas
25	Estrategico	Gestion Gerencial	C-HDW	5202022	PC	Equipo de Computo	Sede Administrativa	Gerente	Cristina Osorio
26	Apoyo	Gestión Contable-Administrativa	C-HDW	5202577	PC	Equipo de Computo	Sede Administrativa	Contadora	Luisa Holguin
27	Misionales	Gestion prestacion de servicios	C-HDW	5202801	PC	Equipo de Computo	Sede Administrativa	Directora Prestacion de Servicios	Laura Yepes
28	Misionales	Gestion prestacion de servicios	C-HDW	5202147	PC	Equipo de Computo	Sede Administrativa	Directora Prestacion de Servicios	Stella Alzate
29	Misionales	Gestion prestacion de servicios	C-HDW	5202820	PC	Equipo de Computo	Sede Administrativa	Directora Prestacion de Servicios	Katy Munera
30	Misionales	Gestion prestacion de servicios	C-HDW	5202731	PC	Equipo de Computo	Sede Administrativa	Directora Prestacion de Servicios	Camila Velez
31	Misionales	Gestion prestacion de servicios	C-HDW	5202544	PC	Equipo de Computo	Sede Administrativa	Directora Prestacion de Servicios	Yuly Grajales
32	Misionales	Gestion prestacion de servicios	C-HDW	5202856	PC	Equipo de Computo	Sede Administrativa	Directora Prestacion de Servicios	Natalia Pareja
33	Apoyo	Gestión de Calidad	C-HDW	5202549	PC	Equipo de Computo	Sede Administrativa	Coord. Calidad	Anna Osa
34	Apoyo	Gestión Contable-Administrativa	C-HDW	5202569	PC	Equipo de Computo	Sede Administrativa	Contadora	Luisa María Loaiza
35	Misionales	Gestion prestacion de servicios	C-HDW	5202347	PC	Equipo de Computo	Sede Administrativa	Directora Prestacion de Servicios	Maria Jose Espitia
36	Apoyo	Gestión Contable-Administrativa	C-HDW	5202737	PC	Equipo de Computo	Sede Administrativa	Contadora	Daniela Ramirez
37	Misionales	Gestion prestacion de servicios	C-HDW	5202510	PC	Equipo de Computo	Sede Administrativa	Directora Prestacion de Servicios	Lizeth Arias
38	Misionales	Gestion prestacion de servicios	C-HDW	5202381	PC	Equipo de Computo	Sede Administrativa	Directora Prestacion de Servicios	Geraldin Viasus
39	Apoyo	Gestión Humana	C-HDW	5202518	PC	Equipo de Computo	Sede Administrativa	Coord. Gestión Humana	Lucy Huertas
40	Apoyo	Gestión Humana	C-HDW	5202525	PC	Equipo de Computo	Sede Administrativa	Coord. Gestión Humana	Oscar Mora

Tabla 3. Continuación tabla 3 Activos 21 al 40. Inventario de activos de información.

Fuente. Elaboración propia

Nro	Proceso	Area o Departamento	Tipo de activo (Servicio/C-SRV, Software/C-SFW, Hardware/C-HDW)	Identificador	Nombre del activo	Descripción del activo	Ubicación fisica	Propietario	Responsable (Custodio)
41	Misionales	Gestion prestacion de servicios	C-HDW	5202132	PC	Equipo de Computo	Sede Administrativa	Directora Prestacion de Servicios	Leidy Paola Jiménez
42	Misionales	Gestion prestacion de servicios	C-HDW	5202651	PC	Equipo de Computo	Sede Administrativa	Directora Prestacion de Servicios	Lorena Grisales
43	Misionales	Gestion prestacion de servicios	C-HDW	5202026	PC	Equipo de Computo	Sede Administrativa	Directora Prestacion de Servicios	Stefany Largo
44	Misionales	Gestion prestacion de servicios	C-HDW	5202048	PC	Equipo de Computo	Sede Administrativa	Directora Prestacion de Servicios	Juan Pablo Cardona
45	Misionales	Gestion prestacion de servicios	C-HDW	5202941	PC	Equipo de Computo	Sede Administrativa	Directora Prestacion de Servicios	Manuela Osorio
46	Misionales	Gestion prestacion de servicios	C-HDW	5202365	PC	Equipo de Computo	Sede Administrativa	Directora Prestacion de Servicios	
47	Apoyo	Gestión de Calidad	C-HDW	5202852	PC	Equipo de Computo	Sede Administrativa	Coord. Calidad	Valentina Grajales
48	Misionales	Gestion Asistencial	C-HDW	5202003	PC	Equipo de Computo	Sede Asistencial	Lider Farmacia	Jennifer Montoya
49	Misionales	Gestion Asistencial	C-HDW	5202013	PC	Equipo de Computo	Sede Asistencial	Coord. Enfermeria	Aux. Enfermeria
50	Misionales	Gestion Asistencial	C-HDW	5202034	PC	Equipo de Computo	Sede Asistencial	Coord. Enfermeria	Aux. Enfermeria
51	Misionales	Gestion Asistencial	C-HDW	5202035	PC	Equipo de Computo	Sede Asistencial	Coord. Enfermeria	Aux. Enfermeria
52	Misionales	Gestion Asistencial	C-HDW	5202037	PC	Equipo de Computo	Sede Asistencial	Coord. Enfermeria	Aux. Enfermeria
53	Misionales	Gestion Asistencial	C-HDW	5202017	PC	Equipo de Computo	Sede Asistencial	Coord. Enfermeria	Aux. Enfermeria
54	Misionales	Gestion Asistencial	C-HDW	5202020	PC	Equipo de Computo	Sede Asistencial	Coord. Enfermeria	Libaniel Bedoya
55	Misionales	Gestion Asistencial	C-HDW	5202016	PC	Equipo de Computo	Sede Asistencial	Lider Central de Esterilizacion	Diana Gonzales
56	Misionales	Gestion Asistencial	C-HDW	5202021	PC	Equipo de Computo	Sede Asistencial	Coord. Enfermeria	Aux. Enfermeria
57	Misionales	Gestion Asistencial	C-HDW	5202765	PC	Equipo de Computo	Sede Asistencial	Coord. Enfermeria	Claudia Quiroz
58	Misionales	Gestion Asistencial	C-HDW	5202341	PC	Equipo de Computo	Sede Asistencial	Coord. Enfermeria	Aux. Enfermeria
59	Misionales	Gestion Asistencial	C-HDW	5202136	PC	Equipo de Computo	Sede Asistencial	Coord. Enfermeria	Alba Lucia Vinasco
60	Misionales	Gestion Asistencial	C-HDW	5202079	PC	Equipo de Computo	Sede Asistencial	Lider M y M	Angela Maria Betancur

Tabla 3. Continuación tabla 3 Activos 41 al 60. Inventario de activos de información.

Fuente. Elaboración propia

Nro	Proceso	Area o Departamento	Tipo de activo (Servicio/C-SRV, Software/C-SFW, Hardware/C-HDW)	Identificador	Nombre del activo	Descripción del activo	Ubicación fisica	Propietario	Responsable (Custodio)
61	Misionales	Gestion Asistencial	C-HDW	5202897	PC	Equipo de Computo	Sede Asistencial	Lider Farmacia	Jhon Mario Peña
62	Misionales	Gestion Asistencial	C-HDW	5202292	PC	Equipo de Computo	Sede Asistencial	Lider Farmacia	Erika Hernandez
63	Misionales	Gestion Asistencial	C-HDW	5202035	PC	Equipo de Computo	Sede Asistencial	Coord. Enfermeria	Yenny Ramirez
64	Misionales	Gestion Asistencial	C-HDW	5202017	PC	Equipo de Computo	Sede Asistencial	Coord. Enfermeria	Monica Maria Perez
65	Misionales	Gestion Asistencial	C-HDW	5202139	PC	Equipo de Computo	Sede Asistencial	Coord. Enfermeria	Natalia Aguirre
66	Misionales	Gestion Asistencial	C-HDW	5202875	PC	Equipo de Computo	Sede Asistencial	Coord. Enfermeria	Libaniel Bedoya
67	Misionales	Gestion Asistencial	C-HDW	5202850	PC	Equipo de Computo	MegaCentro - Consulorio 1110	Directora Prestacion de Servicios	Medico General
68	Misionales	Gestion Asistencial	C-HDW	5202678	PC	Equipo de Computo	MegaCentro - Consulorio 1110	Directora Prestacion de Servicios	Medico General
69	Misionales	Gestion Asistencial	C-HDW	5202455	PC	Equipo de Computo	MegaCentro - Consulorio 1110	Directora Prestacion de Servicios	Lina Garcia
70	Misionales	Gestion Asistencial	C-HDW	5202822	PC	Equipo de Computo	MegaCentro - Consulorio 1110	Directora Prestacion de Servicios	Paula Salgado
71	Misionales	Gestion Asistencial	C-HDW	5202746	PC	Equipo de Computo	MegaCentro - Consultorio 206	Directora Prestacion de Servicios	Monica Colorado
72	Misionales	Gestion Asistencial	C-HDW	5202646	PC	Equipo de Computo	MegaCentro - Consultorio 501	Directora Prestacion de Servicios	Flor Villada
72	Misionales	Gestion Asistencial	C-HDW	5202929	PC	Equipo de Computo	MegaCentro - Consultorio 501	Directora Prestacion de Servicios	Leidy Lotero
73	Misionales	Gestion Asistencial	C-HDW	5202967	PC	Equipo de Computo	MegaCentro - Consultorio 206	Directora Prestacion de Servicios	Jhoana Uribe Moreno
74	Misionales	Gestion Asistencial	C-HDW	5202262	PC	Equipo de Computo	MegaCentro - Consultorio 904	Directora Prestacion de Servicios	Especilista
75	Misionales	Gestion Asistencial	C-HDW	5202912	PC	Equipo de Computo	MegaCentro - Consultorio 904	Directora Prestacion de Servicios	Medico General
76	Misionales	Gestion Asistencial	C-HDW	5202701	PC	Equipo de Computo	MegaCentro - Consultorio 904	Directora Prestacion de Servicios	Jose Andres Serna
77	Misionales	Gestion Asistencial	C-HDW	5202577	PC	Equipo de Computo	MegaCentro - Consultorio 501	Directora Prestacion de Servicios	Mariana Casteña
78	Misionales	Gestion Asistencial	C-HDW	5202501	PC	Equipo de Computo	MegaCentro - Consultorio 501	Directora Prestacion de Servicios	Stefany Largo
79	Misionales	Gestion Asistencial	C-HDW	5202010	PC	Equipo de Computo	Sede Rosales	Directora Prestacion de Servicios	Especialista
80	Misionales	Gestion Asistencial	C-HDW	5202015	PC	Equipo de Computo	Sede2 Armenia - Consultorio	Directora Prestacion de Servicios	Claudia Chavez

Tabla 3. Continuación tabla 3 Activos 61 al 80. Inventario de activos de información.

Fuente. Elaboración propia

Nro	Proceso	Area o Departamento	Tipo de activo (Servicio/C-SRV, Software/C-SFW, Hardware/C-HDW)	Identificador	Nombre del activo	Descripción del activo	Ubicaciòn fisica	Propietario	Responsable (Custodio)
81	Misionales	Gestion Asistencial	C-HDW	5202024	PC	Equipo de Computo	Sede1 Armenia - Consultorio	Directora Prestacion de Servicios	Sandra Saavedra
82	Misionales	Gestion Asistencial	C-HDW	5202026	PC	Equipo de Computo	Sede1 Armenia - Consultorio	Directora Prestacion de Servicios	Aux. Enfermeria
83	Misionales	Gestion Asistencial	C-HDW	5202041	PC	Equipo de Computo	Sede2 Armenia - Consultorio	Directora Prestacion de Servicios	Claudia Diaz
84	Misionales	Gestion Asistencial	C-HDW	5202025	PC	Equipo de Computo	Sede1 Armenia - Consultorio	Directora Prestacion de Servicios	Especialista
85	Misionales	Gestion Asistencial	C-HDW	5202190	PC	Equipo de Computo	Sede2 Armenia - Consultorio	Directora Prestacion de Servicios	Especialista
86	Misionales	Gestion Asistencial	C-HDW	5202356	PC	Equipo de Computo	Sede2 Armenia - Consultorio	Directora Prestacion de Servicios	Paola Quintero
87	Misionales	Gestion Asistencial	C-HDW	5202538	PC	Equipo de Computo	Sede3 Armenia - Consultorio	Directora Prestacion de Servicios	Especialista
88	Misionales	Gestion Asistencial	C-HDW	5202134	PC	Equipo de Computo	Sede2 Armenia - Consultorio	Directora Prestacion de Servicios	Claudia Diaz
89	Misionales	Gestion Asistencial	C-HDW	5202561	PC	Equipo de Computo	Sede1 Armenia - Consultorio	Directora Prestacion de Servicios	Yuly Andrea Triana
90	Misionales	Gestion Asistencial	C-HDW	5202385	PC	Equipo de Computo	Sede3 Armenia - Consultorio	Directora Prestacion de Servicios	Johana Calvo
91	Misionales	Gestion Asistencial	C-HDW	5202897	PC	Equipo de Computo	Sede4 Armenia - Consultorio	Directora Prestacion de Servicios	Especialista
92	Misionales	Gestion Asistencial	C-HDW	5202172	PC	Equipo de Computo	Sede4 Armenia - Consultorio	Directora Prestacion de Servicios	Especialista
93	Misionales	Gestion Asistencial	C-HDW	5202582	PC	Equipo de Computo	Sede4 Armenia - Consultorio	Directora Prestacion de Servicios	Especialista
94	Misionales	Gestion Asistencial	C-HDW	5202348	PC	Equipo de Computo	Satelite - Hospital San	Directora Prestacion de Servicios	Medico
95	Misionales	Gestion Asistencial	C-HDW	5202521	PC	Equipo de Computo	Satelite - Comfamiliar	Directora Prestacion de Servicios	Medico

Tabla 3. Continuación tabla 3 Activos 81 al 96. Inventario de activos de información.

Fuente. Elaboración propia

La tabla a continuación contiene información adicional con detalles más técnicos sobre los activos de información

INVENTARIO DE ACTIVOS DE INFORMACION - DETALLE TECNICO																														
INFORMACION GENERAL								CARACTERISTICAS TECNICAS					CARACTERISTICAS DE GESTION								GESTION SERVIDORES				SISTEMAS DE INFORMACION Y APLICATIVOS					
Identificador	Codigo	Tipo Activo	Oficina	Descripcion	Ubicación	Propietario	Responsable	Marca	Modelo	Serial	Ram	D. Duro	Procesador	Sistema Operativo	Identicador Host	Usuario Admin	Direccion Ip	Direccion MAC	Licencia Antivirus	Vencimiento Antivirus	Protocolo Acc	Puerto Acc	Version Firmware	Rol	Detalle	URL Acceso	Proveedor				
5202999	C-HDW	Hardware	Sede Administrativa	PC	Gestion Humana	Coordinador Gestion Humana	Lucy Huertas	TOSHIBA	S.PRO C650 - SP6005L	GA103205Q	4 GB	320 GB	Intel Core	Windows 7 Professional	aprendiz-calcul	aprendiz	172.168.62.###	00:05:0A:FE:D4:23	HSHJ2-XEJGJ-8M5ZP-RBTNS	6/11/2021	N/A	N/A	N/A	N/A	N/A	N/A	N/A				
5202011	C-HDW	Hardware	Sede Administrativa	PC	Gestion Humana	Coordinador Gestion Humana	Lucy Huertas	HG	HG00471	116688	4 GB	120 GB	Intel Core i3	Windows 10 Pro	ROSCon506	Medicos	172.168.62.###		UKN3X-S66GQ-W1R92-15HKM	23/04/2023	N/A	N/A	N/A	N/A	N/A	N/A				
5202010	C-HDW	Hardware	Sede Rosales	PC	Gestión de Prestacion Servicios	Directora Prestacion de Servicios	Especialista	LENOVO	C20-00	MP13UHNZ	8 GB	120 GB	Intel Quaq Core	Windows 10 Home Single	ROSCon513	Medicos	172.16.2.XXX		TE943-R8WMA-EHAPB-GM7F4	4/12/2023	N/A	N/A	N/A	N/A	N/A	N/A				
5202031	C-HDW	Hardware	Sede Administrativa	PC	Gestion Humana	Coordinador Gestion Humana	Lucy Huertas	LENOVO	S200Z	MP1A5MPT	8 GB	120 GB	Intel Celeron	Windows 10 Pro	ADMAprendiz	aprendiz	172.168.62.###	00:05:0A:FE:D4:86	DMSXK-DKQDV-C2SG9-8YGFP	18/09/2023	N/A	N/A	N/A	N/A	N/A	N/A				
5202003	C-HDW	Hardware	Sede Asistencial	PC	Gestion Asistencial	Lider Farmacia	Jennifer Montoya	LENOVO	G40-80	PF071F65	8 GB	120 GB	Intel Core i3	Windows 10 Home	MEGFarmacia2	deposito	192.168.5.###	00:05:0A:FE:D4:23	K95PE-BFNP7-67B1J-EEP3Z	15/03/2023	N/A	N/A	N/A	N/A	N/A	N/A				
5202007	C-HDW	Hardware	Sede Administrativa	PC	Gestión de Prestacion Servicios	Directora Prestacion de Servicios	Adriana Martinez	LENOVO	G40-80	PF07690R	8 GB	120 GB	Intel Core i3	Windows 10 Home	ADMAsisComercial	auxadmin2	172.168.62.###	00:05:0A:FE:D4:86	J9WK6-QWHGN-6DG4C-V24TN	2/04/2023	N/A	N/A	N/A	N/A	N/A	N/A				
5202013	C-HDW	Hardware	Sede Asistencial	PC	Gestion Asistencial	Coord. Enfermeria	Aux. Enfermeria	LENOVO	G40-80	PF076J8F	4 GB	240 GB	Intel Core i3	Windows 10 Home	MEGRecupera03	Asistencial	192.168.5.###	00:05:0A:FE:D4:23	J9WK6-QWHGN-6DG4C-V24TN	2/04/2023	N/A	N/A	N/A	N/A	N/A	N/A				
5202006	C-HDW	Hardware	Sede Administrativa	PC	Gestión de Prestacion Servicios	Directora Prestacion de Servicios	Supernumerario	COMPUMAX	Compumax	102SN19440	4 GB	120 GB	Intel Celeron	Windows 10 Home	ADMSuper	Medicos	172.168.62.###	00:05:0A:FE:D4:86	J9WK6-QWHGN-6DG4C-V24TN	2/04/2023	N/A	N/A	N/A	N/A	N/A	N/A				
5202005	C-HDW	Hardware	Sede Administrativa	PC	Gestion Contable-Administrativa	Contadora	Tatiana Lopez	HP	14-ck1035la	5CGOO24RD4	8 GB	240 GB	Intel Core i5	Windows 10 Home	ADMContabilidad02	contabilidad	172.168.62.###	00:05:0A:FE:D4:86	UKN3X-S66GQ-W1R92-15HKM	23/04/2023	N/A	N/A	N/A	N/A	N/A	N/A				
5202015	C-HDW	Hardware	Sede2 Armenia - Consultorio 515	PC	Gestión de Prestacion Servicios	Directora Prestacion de Servicios	Claudia Chavez	HP	22-dd1506la	8CC2090R2T	8 GB	256 GB	Intel Core i3	Windows 11 Home Single	ARM2Recepcion2	Armenia2	192..168.2.XXX		DMSXK-DKQDV-C2SG9-8YGFP	18/09/2023	N/A	N/A	N/A	N/A	N/A	N/A				
5202009	C-HDW	Hardware	Sede Administrativa	PC	Gestión de Prestacion Servicios	Directora Prestacion de Servicios	Lorena Puerta	LENOVO	C560	CS01436850	8 GB	120 GB	Intel Core i3	Windows 10 Home	ADMFacturacion1	FACTURACION	172.168.62.###	00:05:0A:FE:D4:86	J9WK6-QWHGN-6DG4C-V24TN	2/04/2023	N/A	N/A	N/A	N/A	N/A	N/A				
5202008	C-HDW	Hardware	Sede Administrativa	PC	Gestión de Prestacion Servicios	Directora Prestacion de Servicios	Juan David Echeverry	ASUS	V221ID	H3PTCJ0137 15	4 GB	128 GB	Intel Pentium	Windows 10 Pro	FACTURACION2	FACTURACION2	172.168.62.###	00:05:0A:FE:D4:86	4JHR8-K2Q7C-8C2GP-YNTRB	10/07/2023	N/A	N/A	N/A	N/A	N/A	N/A				

5202032	C-HDW	Hardware	Sede Asistencial	FIREW ALL	Centro de Datos	Gerente	Apoyo TI	HP	ML110	MX2026005X	12 GB	1000 GB	Intel Core i3	Sopos XG Home Edition		Admin	192.168.65.###	00:05:0A:F E:D4:23	N/A	N/A	HTT PS	####	Sfos 18.5.2 MR-2-	Seguridad Perimetral	Firewall Corporativo	https://181.129.2 27.190:15000		N/A			
5202033	C-HDW	Hardware	Institucional	SERVI DOR	Centro de Datos	Gerente	Cristina Osorio	LENOV O	THINKSERV ER TS140	MJ03RA4U	8 GB	2000 GB	Intel Xeon E3 3.3 Ghz	Win Server Std 2008 R2	Zeus	ADM	172.168.62.###	00:05:0A:F E:D4:86	1WB1V-DN6VU-592KD-T5P5J	23/02/2024	RDP	3389	N/A	N/A	File server		N/A	N/A			
5202014	C-HDW	Hardware	Sede Administrativa	PC	Gestion Gerencial	Gerente	Cristina Osorio	ASUS	K555UQ-DM007	G7N0CV12P 80829B	8 GB	240 GB	Intel Core i7	Windows 10 Pro	ADMGeren cia	gerencia	172.168.62.###	00:05:0A:F E:D4:86	4JHR8-K2Q7C-8C2GP-YNTRB	10/07/2023	N/A	N/A	N/A	N/A	N/A		N/A	N/A			
5202034	C-HDW	Hardware	Sede Asistencial	PC	Gestion Asistencial	Coord. Enfermeria	Aux. Enfermeria	TOSHIB A	S.PRO C650 - SP600SL	7A639617Q	4 GB	120 GB	Intel Core	Windows 10 Home	MEGRecup era01	Medicos	192.168.5.###	00:05:0A:F E:D4:23	1WB1V-DN6VU-592KD-T5P5J	23/02/2024	N/A	N/A	N/A	N/A	N/A		N/A	N/A			
5202029	C-HDW	Hardware	Sede Administrativa	PC	Gestión de Prestacion Servicios	Directora Prestacion de Servicios	Bryan Salas	LENOV O	IDEACENTR E 310-20IAP	YJ009SCC	8 GB	120 GB	Intel Pentium	Windows 10 Home	ADMHistori as	HISTORIA S	172.168.62.###	00:05:0A:F E:D4:86	J9WK6-QWHGN-6DG4C-V24TN	2/04/2023	N/A	N/A	N/A	N/A	N/A		N/A	N/A			
5202048	C-HDW	Hardware	Sede Administrativa	PC	Gestion Humana	Coordinador Gestion Humana	Lucy Huertas	TOSHIB A	SATELLITE C45 A411ZWL	3E151417C	8 GB	128 GB	Intel Celeron	Windows 10 Home	ADMMovil0 1	UserAdmin	172.168.62.###	00:05:0A:F E:D4:86	1WB1V-DN6VU-592KD-T5P5J	23/02/2024	N/A	N/A	N/A	N/A	N/A		N/A	N/A			
5202016	C-HDW	Hardware	Sede Administrativa	PC	Gestión de Prestacion Servicios	Directora Prestacion de Servicios	Isabela Betancur	HP	22-dd1506la	8CC2090Q7 Q	8 GB	256 GB	Intel Core I3	Windows 11 Home Single	ADMFactur acion3	Facturacio n3	172.168.62.###	00:05:0A:F E:D4:86	DMSXK-DKQDV-C2SG9-8YGFP	18/09/2023	N/A	N/A	N/A	N/A	N/A		N/A	N/A			
5202018	C-HDW	Hardware	Sede Administrativa	PC	Gestion Humana	Coordinador Gestion Humana	Lucy Huertas	TOSHIB A	Satellite C45 A411ZWL	3E141417C	4GB	120 GB	Intel Celeron	Windows 10 Home Single	ADMMovil0 2	UserAdmin	172.168.62.###	00:05:0A:F E:D4:86	B5KGV-CAEK8-A5TFD-7GAAD	2/04/2023	N/A	N/A	N/A	N/A	N/A		N/A	N/A			
5202035	C-HDW	Hardware	Sede Asistencial	PC	Gestion Asistencial	Coord. Enfermeria	Aux. Enfermeria	TOSHIB A	Satellite C45 A411ZWL	3E144755C	4 GB	120 GB	Intel Celeron	Windows 10 Home	MEGRecup era04	AuxAsis	192.168.5.###	00:05:0A:F E:D4:23	TE943-R8WMA-EHAPB-GM7F4	4/12/2023	N/A	N/A	N/A	N/A	N/A		N/A	N/A			
5202037	C-HDW	Hardware	Sede Asistencial	PC	Gestion Asistencial	Coord. Enfermeria	Aux. Enfermeria	TOSHIB A	Satellite C45 A411ZWL	3E151389C	4 GB	500 GB	Intel Celeron	Windows 10 Pro	MEGQuirof ano2	Asistencial	192.168.5.###	00:05:0A:F E:D4:23	4JHR8-K2Q7C-8C2GP-YNTRB	10/07/2023	N/A	N/A	N/A	N/A	N/A		N/A	N/A			
5202017	C-HDW	Hardware	Sede Asistencial	PC	Gestion Asistencial	Coord. Enfermedia	Aux. Enfermeria	HP	14-cf2518la	5CG14926P3	8 GB	256 GB	Intel Core i3	Windows 11 Home Single	MEGQuirof ano1	AuxAsis	192.168.5.###	00:05:0A:F E:D4:23	J9WK6-QWHGN-6DG4C-V24TN	2/04/2023	N/A	N/A	N/A	N/A	N/A		N/A	N/A			
5202020	C-HDW	Hardware	Sede Asistencial	PC	Gestion Asistencial	Coord. Enfermedia	Libaniel Bedoya	HP	14-r215la	CND52227Z W	8 GB	120 GB	Intel Core i3	Windows 10 Home	MEGRecep cion02	recepcion2	192.168.5.###	00:05:0A:F E:D4:23	K95PE-BFNP7-67B1J-EEP3Z	15/03/2023	N/A	N/A	N/A	N/A	N/A		N/A	N/A			
5202016	C-HDW	Hardware	Sede Asistencial	PC	Gestion Asistencial	Lider Central de Esterilizacion	Diana Gonzales	HP	14-ck1035la	5CG0024S4J	8 GB	240 GB	Intel Core i5	Windows 10 Home	CLCMEGHI S01	Central	192.168.5.###	00:05:0A:F E:D4:23	UKN3X-S66GQ-W1R92-15HKM	23/04/2023	N/A	N/A	N/A	N/A	N/A		N/A	N/A			
5202021	C-HDW	Hardware	Sede Asistencial	PC	Gestion Asistencial	Coord. Enfermeria	Aux. Enfermeria	HG	Torre HG	114939	8 GB	120 GB	Intel Celeron	Windows 10 Pro	MEGRecup era05	medicos	192.168.5.###	00:05:0A:F E:D4:23	TE943-R8WMA-EHAPB-GM7F4	4/12/2023	N/A	N/A	N/A	N/A	N/A		N/A	N/A			
5202024	C-HDW	Hardware	Sede1 Armenia - Consultorio 513	PC	Gestión de Prestacion Servicios	Directora Prestacion de Servicios	Sandra Saavedra	HP	22-c014LA	8CC91758C2	4 GB	240 GB	Intel Core i3	Windows 10 Home Single	ARM1Rece pcion	Armenia	192.168.0.XXX		UKN3X-S66GQ-W1R92-15HKM	23/04/2023	N/A	N/A	N/A	N/A	N/A		N/A	N/A			
5202026	C-HDW	Hardware	Sede1 Armenia - Consultorio 513	PC	Gestión de Prestacion Servicios	Directora Prestacion de Servicios	Aux. Enfermeria	DELL	Inspiron 14-3467	88JZBL2	8 GB	128 GB	Intel Core i3	Windows 10 Pro	ARM1Cirugi a	Armenia5	192.168.0.XXX		TE943-R8WMA-EHAPB-GM7F4	4/12/2023	N/A	N/A	N/A	N/A	N/A		N/A	N/A			
5202041	C-HDW	Hardware	Sede2 Armenia - Consultorio 515	PC	Gestión de Prestacion Servicios	Directora Prestacion de Servicios	Claudia Diaz	COMPU MAX	EQ COMPUMAX	300SN43768	4 GB	500 GB	Intel Celeron	Windows 10 Pro	ARM2Urodi namia	Usuario	192..168.2.XXX		TE943-R8WMA-EHAPB-GM7F4	4/12/2023	N/A	N/A	N/A	N/A	N/A		N/A	N/A			
5202025	C-HDW	Hardware	Sede1 Armenia - Consultorio 513	PC	Gestión de Prestacion Servicios	Directora Prestacion de Servicios	Especialist a	HP	22-c014LA	8CC91758J0	4 GB	120 GB	Intel Core3	Windows 10 Home	ARM1Cons ultorio	Medicos	192.168.0.XXX		TE943-R8WMA-EHAPB-GM7F4	4/12/2023	N/A	N/A	N/A	N/A	N/A		N/A	N/A			
5202022	C-HDW	Hardware	Sede Administrativa	PC	Gestion Gerencial	Gerente	Cristina Osorio	HP	14-ck1035la	5CG0024S25	8 GB	240 GB	Intel Core i5	Windows 10 Home	ADMGeren ciaMovil	Gerencia	172.168.62.###	00:05:0A:F E:D4:86	UKN3X-S66GQ-W1R92-15HKM	23/04/2023	N/A	N/A	N/A	N/A	N/A		N/A	N/A			
5202765	C-HDW	Hardware	Sede Asistencial	PC	Gestion Asistencial	Coord. Enfermeria	Claudia Quiroz	DELL	Vostro 14	25953065606	8 GB	120 GB	Intel Core i3	Windows 10 Pro	MEGEnfJef e1	Asistencial	192.168.5.###	00:05:0A:F E:D4:23	K95PE-BFNP7-67B1J-EEP3Z	15/03/2023	N/A	N/A	N/A	N/A	N/A		N/A	N/A			
5202577	C-HDW	Hardware	Sede Administrativa	PC	Gestion Contable-Administrativa	Contadora	Luisa Holguin	HP	15-dw1056la	CND0385X81	8 GB	240 GB	Intel Core i5	Windows 10 Home Single	CLCCONJ EF	administra dora	172.168.62.###	00:05:0A:F E:D4:86	1WB1V-DN6VU-592KD-T5P5J	23/02/2024	N/A	N/A	N/A	N/A	N/A		N/A	N/A			
5202801	C-HDW	Hardware	Sede Administrativa	PC	Gestión de Prestacion Servicios	Directora Prestacion de Servicios	Laura Yepes	LENOV O	IdeaCentre A340-22AST	MP1TR0X8	8 GB	1000 GB	AMD A9-9425	Windows 10 Home Single	ADMCallCe nter04	CallCenter 4	172.168.62.###	00:05:0A:F E:D4:86	UKN3X-S66GQ-W1R92-15HKM	23/04/2023	N/A	N/A	N/A	N/A	N/A		N/A	N/A			
5202341	C-HDW	Hardware	Sede Asistencial	PC	Gestion Asistencial	Coord. Enfermeria	Aux. Enfermeria	LENOV O	IdeaCentre A340-22AST	MP1TQZCR	8 GB	1000 GB	AMD A9-9425	Windows 10 Home	MEGRecup era02	Medicos	192.168.5.###	00:05:0A:F E:D4:23	SA1UW-5UX8C-8A3W6-6W6MY	23/10/2023	N/A	N/A	N/A	N/A	N/A		N/A	N/A			
5202190	C-HDW	Hardware	Sede2 Armenia - Consultorio 515	PC	Gestión de Prestacion Servicios	Directora Prestacion de Servicios	Especialist a	HP	24-df0020LA	8CC1101L75	4 GB	1240 GB	Intel Pentium Silver	Windows 10 Home	ARM2Cons ultorio	Medicos	192..168.2.XXX		1WB1V-DN6VU-592KD-T5P5J	23/02/2024	N/A	N/A	N/A	N/A	N/A		N/A	N/A			

5202356	C-HDW	Hardware	Sede2 Armenia - Consultorio 515	PC	Gestión de Prestacion Servicios	Directora Prestacion de Servicios	Paola Quintero	HP	24-df0020LA	8CC1101L68	4 GB	1240 GB	Intel Pentium Silver	Windows 10 Home	ARM2Recepcion	Medicos	192..168.2.XXX		UKN3X-S66GQ-W1R92-15HKM	23/04/2023	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5202147	C-HDW	Hardware	Sede Administrativa	PC	Gestión de Prestacion Servicios	Directora Prestacion de Servicios	Stella Alzate	HP	24-df0020LA	8CC1101KYR	4 GB	1240 GB	Intel Pentium Silver	Windows 10 Home Single	ADMCallCenter05	CallCenter5	172.168.62.###	00:05:0A:FE:D4:86	UKN3X-S66GQ-W1R92-15HKM	23/04/2023	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5202136	C-HDW	Hardware	Sede Asistencial	PC	Gestion Asistencial	Coord. Enfermeria	Alba Lucia Vinasco	HP	24-df0020LA	8CC11207M2	4 GB	1240 GB	AMD Ryzen 3	Windows 10 Home Single	MEGRecepcion01	Recepcion	192.168.5.###	00:05:0A:FE:D4:23	J9WK6-QWHGN-6DG4C-V24TN	2/04/2023	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5202820	C-HDW	Hardware	Sede Administrativa	PC	Gestión de Prestacion Servicios	Directora Prestacion de Servicios	Katy Munera	HP	14-cf2067la	5CG1116WS5	8 GB	240 GB	Intel Core I3	Windows 10 Home Single	ADMDirCo mercial	DIRECCION	172.168.62.###	00:05:0A:FE:D4:86	J9WK6-QWHGN-6DG4C-V24TN	2/04/2023	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5202538	C-HDW	Hardware	Sede3 Armenia - Consultorio 512	PC	Gestión de Prestacion Servicios	Directora Prestacion de Servicios	Especialista	HP	24-df0020LA	8CC1150WR3	4 GB	1240 GB	AMD Ryzen 3	Windows 10 Home Single	ARM3Consultorio	Medicos	192.168.0.XXX		DMSXK-DKQDV-C2SG9-8YGFP	18/09/2023	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5202850	C-HDW	Hardware	MegaCentro - Consulorio 1110	PC	Gestión de Prestacion Servicios	Directora Prestacion de Servicios	Medico General	HP	24-df0020LA	8CC113OPLQ	4 GB	1240 GB	AMD Ryzen 3	Windows 10 Home Single	MEG904Con01	Medicos	192.168.1.#		ED62X-P4B8U-VSX8S-WPKJE	2/11/2023	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5202678	C-HDW	Hardware	MegaCentro - Consulorio 1110	PC	Gestión de Prestacion Servicios	Directora Prestacion de Servicios	Medico General	HP	24-df0020LA	8CC1130PLR	4 GB	1240 GB	AMD Ryzen 3	Windows 10 Home Single	MEG904Con02	Medicos	192.168.1.#		ED62X-P4B8U-VSX8S-WPKJE	2/11/2023	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5202455	C-HDW	Hardware	MegaCentro - Consulorio 1110	PC	Gestión de Prestacion Servicios	Directora Prestacion de Servicios	Lina Garcia	HP	24-df0020LA	8CC1130PL6	4 GB	1240 GB	AMD Ryzen 3	Windows 10 Home Single	MEG904Sec02	Secretaria 2	192.168.1.#		ED62X-P4B8U-VSX8S-WPKJE	2/11/2023	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5202822	C-HDW	Hardware	MegaCentro - Consulorio 1110	PC	Gestión de Prestacion Servicios	Directora Prestacion de Servicios	Paula Salgado	HP	14-cf2067la	5CG1248X7Q	8 GB	240 GB	Intel Core I3	Windows 10 Home Single	MEG904Sec01	Secretaria 1	192.168.1.#		ED62X-P4B8U-VSX8S-WPKJE	2/11/2023	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5202079	C-HDW	Hardware	Sede Asistencial	PC	Gestion Asistencial	Lider M y M	Angela Maria Betancur	HP	14-cf2067la	5CG1249DTW	8 GB	240 GB	Intel Core I3	Windows 10 Home Single	MEGBiomedico1	Biomedico	192.168.5.###	00:05:0A:FE:D4:23	ED62X-P4B8U-VSX8S-WPKJE	2/11/2023	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5202897	C-HDW	Hardware	Sede Asistencial	PC	Gestion Asistencial	Lider Farmacia	Jhon Mario Peña	HP	14-cf2067la	5CG12957L0	8 GB	240 GB	Intel Core I3	Windows 10 Home Single	MEGCompras1	Compras	192.168.5.###	00:05:0A:FE:D4:23	4JHR8-K2Q7C-8C2GP-YNTRB	10/07/2023	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5202731	C-HDW	Hardware	Sede Administrativa	PC	Gestión de Prestacion Servicios	Directora Prestacion de Servicios	Camila Velez	HP	24-dd0017la	8CC13031R5	4 GB	1240 GB	AMD Ryzen 3	Windows 10 Home Single	ADMCallCenter06	CallCenter6	172.168.62.###	00:05:0A:FE:D4:86	DMSXK-DKQDV-C2SG9-8YGFP	18/09/2023	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

5202356	C-HDW	Hardware	Sede2 Armenia - Consultorio 515	PC	Gestión de Prestacion Servicios	Directora Prestacion de Servicios	Paola Quintero	HP	24-df0020LA	8CC1101L68	4 GB	1240 GB	Intel Pentium Silver	Windows 10 Home	ARM2Recepcion	Medicos	192..168.2.XXX		UKN3X-S66GQ-W1R92-15HKM	23/04/2023	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5202147	C-HDW	Hardware	Sede Administrativa	PC	Gestión de Prestacion Servicios	Directora Prestacion de Servicios	Stella Alzate	HP	24-df0020LA	8CC1101KYR	4 GB	1240 GB	Intel Pentium Silver	Windows 10 Home Single	ADMCallCenter05	CallCenter5	172.168.62.###	00:05:0A:FE:D4:86	UKN3X-S66GQ-W1R92-15HKM	23/04/2023	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5202136	C-HDW	Hardware	Sede Asistencial	PC	Gestion Asistencial	Coord. Enfermeria	Alba Lucia Vinasco	HP	24-df0020LA	8CC11207M2	4 GB	1240 GB	AMD Ryzen 3	Windows 10 Home Single	MEGRecepcion01	Recepcion	192.168.5.###	00:05:0A:FE:D4:23	J9WK6-QWHGN-6DG4C-V24TN	2/04/2023	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5202820	C-HDW	Hardware	Sede Administrativa	PC	Gestión de Prestacion Servicios	Directora Prestacion de Servicios	Katy Munera	HP	14-cf2067la	5CG1116WS5	8 GB	240 GB	Intel Core I3	Windows 10 Home Single	ADMDirCo mercial	DIRECCION	172.168.62.###	00:05:0A:FE:D4:86	J9WK6-QWHGN-6DG4C-V24TN	2/04/2023	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5202538	C-HDW	Hardware	Sede3 Armenia - Consultorio 512	PC	Gestión de Prestacion Servicios	Directora Prestacion de Servicios	Especialista	HP	24-df0020LA	8CC1150WR3	4 GB	1240 GB	AMD Ryzen 3	Windows 10 Home Single	ARM3Consultorio	Medicos	192.168.0.XXX		DMSXK-DKQDV-C2SG9-8YGFP	18/09/2023	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5202850	C-HDW	Hardware	MegaCentro - Consulorio 1110	PC	Gestión de Prestacion Servicios	Directora Prestacion de Servicios	Medico General	HP	24-df0020LA	8CC113OPLQ	4 GB	1240 GB	AMD Ryzen 3	Windows 10 Home Single	MEG904Con01	Medicos	192.168.1.#		ED62X-P4B8U-VSX8S-WPKJE	2/11/2023	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5202678	C-HDW	Hardware	MegaCentro - Consulorio 1110	PC	Gestión de Prestacion Servicios	Directora Prestacion de Servicios	Medico General	HP	24-df0020LA	8CC1130PLR	4 GB	1240 GB	AMD Ryzen 3	Windows 10 Home Single	MEG904Con02	Medicos	192.168.1.#		ED62X-P4B8U-VSX8S-WPKJE	2/11/2023	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5202455	C-HDW	Hardware	MegaCentro - Consulorio 1110	PC	Gestión de Prestacion Servicios	Directora Prestacion de Servicios	Lina Garcia	HP	24-df0020LA	8CC1130PL6	4 GB	1240 GB	AMD Ryzen 3	Windows 10 Home Single	MEG904Sec02	Secretaria 2	192.168.1.#		ED62X-P4B8U-VSX8S-WPKJE	2/11/2023	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5202822	C-HDW	Hardware	MegaCentro - Consulorio 1110	PC	Gestión de Prestacion Servicios	Directora Prestacion de Servicios	Paula Salgado	HP	14-cf2067la	5CG1248X7Q	8 GB	240 GB	Intel Core I3	Windows 10 Home Single	MEG904Sec01	Secretaria 1	192.168.1.#		ED62X-P4B8U-VSX8S-WPKJE	2/11/2023	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5202079	C-HDW	Hardware	Sede Asistencial	PC	Gestion Asistencial	Lider M y M	Angela Maria Betancur	HP	14-cf2067la	5CG1249DTW	8 GB	240 GB	Intel Core I3	Windows 10 Home Single	MEGBiomedico1	Biomedico	192.168.5.###	00:05:0A:FE:D4:23	ED62X-P4B8U-VSX8S-WPKJE	2/11/2023	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5202897	C-HDW	Hardware	Sede Asistencial	PC	Gestion Asistencial	Lider Farmacia	Jhon Mario Peña	HP	14-cf2067la	5CG12957L0	8 GB	240 GB	Intel Core I3	Windows 10 Home Single	MEGCompras1	Compras	192.168.5.###	00:05:0A:FE:D4:23	4JHR8-K2Q7C-8C2GP-YNTRB	10/07/2023	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5202731	C-HDW	Hardware	Sede Administrativa	PC	Gestión de Prestacion Servicios	Directora Prestacion de Servicios	Camila Velez	HP	24-dd0017la	8CC13031R5	4 GB	1240 GB	AMD Ryzen 3	Windows 10 Home Single	ADMCallCenter06	CallCenter6	172.168.62.###	00:05:0A:FE:D4:86	DMSXK-DKQDV-C2SG9-8YGFP	18/09/2023	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

5202967	C-HDW	Hardware	MegaCentro - Local 206B	PC	Gestión de Prestacion Servicios	Directora Prestacion de Servicios	Jhoana Uribe Moreno	HP	22-dd1506la	8CC2090Q8K	8 GB	256 GB	Intel Core i3	Windows 11 Home Single	MEG206Co n01	Medicos	192.168.2.#		J9WK6-QWHGN-6DG4C-V24TN	2/04/2023	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5202347	C-HDW	Hardware	Sede Administrativa	PC	Gestión de Prestacion Servicios	Directora Prestacion de Servicios	Maria Jose Espitia	HP	22-dd1506la	8CC2090Q8X	8 GB	256 GB	Intel Core i3	Windows 11 Home Single	ADMCallCe nter03	CallCenter 3	172.168.62.###	00:05:0A:F E:D4:86	PK32W-B8DR8-JXK9W-ZA25G	19/08/2023	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5202737	C-HDW	Hardware	Sede Administrativa	PC	Gestion Contable-Administrativa	Contadora	Daniela Ramirez	HP	24-dd0506la	8CC212585V	8 GB	256 GB	AMD Ryzen 3	Windows 11 Home Single	ADMConta bilidad01	AuxCont	172.168.62.###	00:05:0A:F E:D4:86	UKN3X-S66GQ-W1R92-1SHKM	23/04/2023	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5202510	C-HDW	Hardware	Sede Administrativa	PC	Gestión de Prestacion Servicios	Directora Prestacion de Servicios	Lizeth Arias	HP	24-dd0506la	8CC2125839	8 GB	256 GB	AMD Ryzen 3	Windows 11 Home Single	ADMCallCe nter07	CallCenter 7	172.168.62.###	00:05:0A:F E:D4:86	PK32W-B8DR8-JXK9W-ZA25G	19/08/2023	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5202262	C-HDW	Hardware	MegaCentro - Consultorio 904	PC	Gestión de Prestacion Servicios	Directora Prestacion de Servicios	Especilista	HP	24-dd0506la	8CC21258RC	8 GB	256 GB	AMD Ryzen 3	Windows 11 Home Single	MEG904Co n03	Medicos	192.168.4.#		SA1UW-SUXBC-8A3W6-6W8MY	23/10/2023	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5202912	C-HDW	Hardware	MegaCentro - Consultorio 904	PC	Gestión de Prestacion Servicios	Directora Prestacion de Servicios	Medico General	HP	24-dd0506la	8CC1501WC N	8 GB	256 GB	AMD Ryzen 3	Windows 11 Home Single	MEG904Co n04	Medicos	192.168.4.#		SA1UW-SUXBC-8A3W6-6W8MY	23/10/2023	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5202701	C-HDW	Hardware	MegaCentro - Consultorio 904	PC	Gestión de Prestacion Servicios	Directora Prestacion de Servicios	Jose Andres Serna	HP	24-dd0506la	8CC1501VY4	8 GB	256 GB	AMD Ryzen 3	Windows 11 Home Single	MEG904Se c03	Secretaria 1	192.168.4.#		SA1UW-SUXBC-8A3W6-6W8MY	23/10/2023	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5202381	C-HDW	Hardware	Sede Administrativa	PC	Gestión de Prestacion Servicios	Directora Prestacion de Servicios	Geraldin Viasus	HP	24-dd0506la	8CC21258C4	8 GB	256 GB	AMD Ryzen 3	Windows 11 Home Single	ADMCallCe nter08	CallCenter 8	172.168.62.###	00:05:0A:F E:D4:86	PK32W-B8DR8-JXK9W-ZA25G	19/08/2023	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5202348	C-HDW	Hardware	Satelite - Hospital San Jorge	PC	Gestión de Prestacion Servicios	Directora Prestacion de Servicios	Medico	HP	14-cf2518la	5CG14925RF	8 GB	256 GB	Intel Core i3	Windows 11 Home Single	SATProfe0 1	Medicos	10.10.1.XXX		SA1UW-SUXBC-8A3W6-6W8MY	23/10/2023	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5202521	C-HDW	Hardware	Satelite - Comfamiliar Risaralda	PC	Gestión de Prestacion Servicios	Directora Prestacion de Servicios	Medico	HP	14-cf2518la	5CG1447HP H	8 GB	256 GB	Intel Core i3	Windows 11 Home Single	SATProfe0 2	Medicos	10.10.2.XXX		SA1UW-SUXBC-8A3W6-6W8MY	23/10/2023	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5202518	C-HDW	Hardware	Sede Administrativa	PC	Gestion Humana	Coordinador Gestion Humana	Lucy Huertas	HP	14-cf2518la	5CG14925PS	8 GB	256 GB	Intel Core i3	Windows 11 Home Single	ADMTHum ano	AsisAdmin	172.168.62.###	00:05:0A:F E:D4:86	J9WK6-QWHGN-6DG4C-V24TN	2/04/2023	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5202525	C-HDW	Hardware	Sede Administrativa	PC	Gestion Humana	Coordinador Gestion Humana	Oscar Mora	HP	14-cf2518la	5CG1492613	8 GB	256 GB	Intel Core i3	Windows 11 Home Single	ADMASisS gi	ASisSgi	172.168.62.###	00:05:0A:F E:D4:86	B5KGV-CAEK8-A5TFD-7GAAD	2/04/2023	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5202385	C-HDW	Hardware	Sede3 Armenia - Consultorio 512	PC	Gestión de Prestacion Servicios	Directora Prestacion de Servicios	Johana Calvo	HP	24-dd0506la	8CC2125888	8 GB	256 GB	AMD Ryzen 3	Windows 11 Home Single	ARM3Auxili ar1	Armenia	192.168.0.XXX		B5KGV-CAEK8-A5TFD-7GAAD	2/04/2023	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5202897	C-HDW	Hardware	Sede4 Armenia - Consultorio 510	PC	Gestión de Prestacion Servicios	Directora Prestacion de Servicios	Especialist a	HP	24-dd0506la	8CC21258TV	8 GB	256 GB	AMD Ryzen 3	Windows 11 Home Single	ARM4Con0 1	Medicos	192.168.0.XXX		ED62X-P4B8U-VSX8S-WPKJE	2/11/2023	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5202172	C-HDW	Hardware	Sede4 Armenia - Consultorio 510	PC	Gestión de Prestacion Servicios	Directora Prestacion de Servicios	Especialist a	HP	24-dd0506la	8CC2125881	8 GB	256 GB	AMD Ryzen 3	Windows 11 Home Single	ARM4Con0 2	Medicos	192.168.0.XXX		ED62X-P4B8U-VSX8S-WPKJE	2/11/2023	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5202582	C-HDW	Hardware	Sede4 Armenia - Consultorio 510	PC	Gestión de Prestacion Servicios	Directora Prestacion de Servicios	Especialist a	HP	24-dd0506la	8CC14200Q6 F	8 GB	256 GB	AMD Ryzen 3	Windows 11 Home Single	ARM4Con0 3	Medicos	192		ED62X-P4B8U-VSX8S-WPKJE	2/11/2023	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5202132	C-HDW	Hardware	Sede Administrativa	PC	Gestión de Prestacion Servicios	Directora Prestacion de Servicios	Leidy Paola Jiménez	HP	22-df1510la	8CC3360RX0	8 GB	256 GB	Intel Core i3	Windows 11 Home Single	ADMSuper 03	Useradmin	172.168.62.###	00:05:0A:F E:D4:86	ZV7G8-G9CAT-SJJGZ-QDS6F	28/02/2024	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5202577	C-HDW	Hardware	MegaCentro - Consultorio 501	PC	Gestión de Prestacion Servicios	Directora Prestacion de Servicios	Mariana Casteña	HP	22-df1510la	8CC2260RQ C	8 GB	256 GB	Intel Core i3	Windows 11 Home Single	MEG501Se c01	Rosales	192.168.3.#		1WB1V-DN6VU-592KD-T5P5J	23/02/2024	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5202651	C-HDW	Hardware	Sede Administrativa	PC	Gestión de Prestacion Servicios	Directora Prestacion de Servicios	Lorena Grisales	HP	22-df1510la	8CC2260S20	8 GB	256 GB	Intel Core i3	Windows 11 Home Single	ADMFactur acion4	Facturacio n4	172.168.62.###	00:05:0A:F E:D4:86	ZV7G8-G9CAT-SJJGZ-QDS6F	28/02/2024	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5202501	C-HDW	Hardware	MegaCentro - Consultorio 501	PC	Gestión de Prestacion Servicios	Directora Prestacion de Servicios	Especialista	HP	22-df1510la	8CC2260RZ0	8 GB	256 GB	Intel Core i3	Windows 11 Home Single	MEG501Co n01	Medicos	192.168.3.#		ED62X-P4B8U-VSX8S-WPKJE	2/11/2023	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5202026	C-HDW	Hardware	Sede Administrativa	PC	Gestión de Prestacion Servicios	Directora Prestacion de Servicios	Stefany Largo	HP	22-df1510la	8CC2260RTS	8 GB	256 GB	Intel Core i3	Windows 11 Home Single	ADMCallCe nter10	CallCenter 10	172.168.62.###	00:05:0A:F E:D4:86	ZV7G8-G9CAT-SJJGZ-QDS6F	28/02/2024	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5202048	C-HDW	Hardware	Sede Administrativa	PC	Gestión de Prestacion Servicios	Directora Prestacion de Servicios	Juan Pablo Cardona	HP	22-df1510la	8CC2260RTT	8 GB	256 GB	Intel Core i3	Windows 11 Home Single	ADMCallCe nter09	CallCenter 9	172.168.62.###	00:05:0A:F E:D4:86	ZV7G8-G9CAT-SJJGZ-QDS6F	28/02/2024	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5202941	C-HDW	Hardware	Sede Administrativa	PC	Gestión de Prestacion Servicios	Directora Prestacion de Servicios	Manuela Osorio	HP	22-df1510la	8CC2260RS X	8 GB	256 GB	Intel Core i3	Windows 11 Home Single	ADMCallCe nter11	CallCenter 11	172.168.62.###	00:05:0A:F E:D4:86	ZV7G8-G9CAT-SJJGZ-QDS6F	28/02/2024	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5202875	C-HDW	Hardware	Sede Asistencial	PC	Gestion Asistencial	Coord. Enfermeria	Libaniel Bedoya	HP	22-df1510la	8CC2260RS K	8 GB	256 GB	Intel Core i3	Windows 11 Home Single	MEGRecep cion02	recepcion2	192.168.5.###	00:05:0A:F E:D4:23			N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

5202365	C-HDW	Hardware	Sede Administrativa	PC	Gestión de Prestacion Servicios	Directora Prestacion de Servicios		HP	22-dd535la	8CC22222XV	8 GB	256 GB	AMD Ryzen 3	Windows 11 Home Single	ADMProgramacion01	ProgramacionO1	172.168.62.###	00:05:0A:FE:D4:86			N/A	N/A	N/A	N/A	N/A	N/A	N/A
5202852	C-HDW	Hardware	Sede Administrativa	PC	Gestion Calidad	Coordinadora Calidad	Valentina Grajales	HP	22-dd535la	8CC22222XT	8 GB	256 GB	AMD Ryzen 3	Windows 11 Home Single	ADMAsisCalidad01	AuxCalidad	172.168.62.###	00:05:0A:FE:D4:86	TE943-R8WMA-EHAPB-GM7F4	4/12/2023	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5202857	C-HDW	Hardware	Sede Administrativa	FIREWALL	Centro de Datos	Gerente	Cristina Osorio	SOPHOS	SF01V	C01001EHW D23RB7	N/A	N/A	N/A	N/A	N/A	Admin	172.168.62.###	00:05:0A:FE:D4:86	N/A	N/A	HTTPS	####	N/A	Stos 17.5.14 rw-14-1	Seguridad Perimetral	Firewall Corporativo	https://172.168.6#:15000	N/A
8080111	C-SFW	Software	Institucional	HIS / ISalud ERP /	Software Nube (DataCenter Tier 3)	Gerente	Apoyo TI	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	HIS (Hospital Informatio	Sistema Gestion Medica	https://calculaserisalud.co	GI+d
8080112	C-SFW	Software	Sede Administrativa	Yeminus	Software Nube (DataCenter Tier 3)	Contadora	Luisa Holguin	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	RDP	8025	N/A	ERP	Sistema Gestion Financier	app.yeminus.com	Yeminus SAS
8080113	C-HDW	Hardware	Institucional	TELEFONIA IP -	Software Nube (DataCenter Tier 3)	Gerente	Apoyo TI	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Telefonia IP	Plataforma de Telefonia	66.175.209.97	Ikono Telecomunica
8080114	C-SRV	Servicios	Sede Administrativa	Call Center - Ikono	Software Nube (DataCenter Tier 3)	Directora Prestacion de Servicios	Katy Munera	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	HTTP	N/A	N/A	Call Center	Plataforma de Call Center	http://66.175.209.97/reportes	Ikono Telecomunica TEK
8080115	C-SFW	Software	Institucional	Kaspersky	En Premisas	Gerente	Apoyo TI	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	HTTPS	N/A	N/A	Antivirus	Solucion Antivirus	https://ksos.kaspersky.com	Soluciones
8080116	C-SRV	Servicios	Institucional	Correo - Google Worksp	Software Nube	Gerente	Apoyo TI	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	HTTPS	N/A	N/A	Correo Electronico	Solucion Correo y Colabora		Nuva
8080117	C-SFW	Software	Institucional	Microsoft 365 APP	En Premisas	Gerente	Apoyo TI	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Ofimatica	Solucion Ofimatica		Movistar
8080118	C-SRV	Servicios	Institucional	Portal Corporativo	Software Nube	Coordinadora Calidad	Ana Marcela Ossa	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	HTTPS	N/A	N/A	Web	Portal Corporativo	https://www.calculaser.com	OkWeb
8080119	C-SRV	Servicios	Institucional	Plexo	Software Nube	Coordinador Talento Humano	Lucy Huertas	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	HTTPS	N/A	N/A	Capacitacion	Plataforma de Capacita	https://capacitorresoft.co/login.php?bx=7	TorreSoft

Tabla 4. Inventario de Activos - Detalle Técnico

Fuente. Elaboración propia

11.2 Valoración de Activos

Corresponde a la asignación de una valor cualitativo o cuantitativo al activo en función de las características o atributos que este posee y que lo convierte en valioso para la organización de esta manera se utilizó las dimensiones propuestas por ISO 27001:2013 que son: confidencialidad, integridad y disponibilidad

Para realizar la valoración de los activos se realizó una mesa de trabajo con los líderes de los procesos estratégicos, misionales y de apoyo que están involucrados con cada activo debido a que conocen a profundidad el significado que cada uno tiene dentro del modelo de negocio que maneja Calculaser SA y como perjudica a la continuidad de la entidad si este llegara a sufrir algún daño.

A fin de obtener una calificación correcta, se plantearon los siguientes interrogantes por cada una de las dimisiones a calificar:

- **Confidencialidad:** ¿Cómo afectaría a Calculaser SA que la información sea conocida por personas ajenas no autorizadas?
- **Integridad**: ¿Cuál sería el daño para la Calculaser SA si un activo estuviera corrupto?
- D**isponibilidad:** ¿Cómo afectaría a Calculaser SA que un activo no pueda ser utilizado?

La siguiente tabla ilustra los valores de referencia para medir el impacto

TABLA PARA VALORACION DE LOS ACTIVOS		
RANGO	IMPACTO	DESCRIPCIÓN
9-10	Extremo	Daño extremadamente grave
7-8	Muy alto	Daño muy grave
6 - 7	Alto	Daño grave
3 - 5	Medio	Daño importante
1 - 2	Bajo	Daño menor

Tabla 5. Escala de valoración activos

Fuente. Elaboración propia

Después de establecer la escala de valoración de activos, se procede a calificar cada activo basado en las preguntas sobre las dimensiones (confidencialidad, integridad y disponibilidad) a calificar. Los resultados más significativos obtenidos son: el HIS/ISALUD con un valor 10.00, el SERVIDOR (Zeus) con un valor de 9,33, el CALL CENTER con un valor de 9,00, el FIREWALL(ASIS/ADM) y CORREO con un valor de 8.67 como se puede observar en la siguiente tabla:

VALORACIÓN DE LOS ACTIVOS DE INFORMACIÓN					
Tipo Activo	Activo	Valoración del Impacto C: Confidencialidad. I: Integridad D: Disponibilidad			
		Confidencialidad	Integridad	Disponibilidad	Total
		¿Cómo afectaría a Calculaser SA que la información sea conocida por personas ajenas no autorizadas?	¿Cuál sería el daño para Calculaser si un activo estuviera corrupto?	¿Cómo afectaría a Calculaser SA que un activo no pueda ser utilizado?	
C-HDW	PC	8	1	1	3,33
C-HDW	SERVIDOR (ZEUS)	10	8	10	9,33
C-HDW	FIREWALL (ADM)	6	10	10	8,67
C-HDW	FIREWALL (ASIS)	6	10	10	8,67
C-HDW	TELEFONIA IP - IKONO PBX	2	2	8	4,00
C-SFW	KASPERSKY SSO	2	2	2	2,00
C-SFW	MICROSOFT 365 APP	2	2	2	2,00
C-SFW	HIS / ISALUD	10	10	10	10,00
C-SFW	ERP/ YEMINUS	5	8	7	6,67
C-SFW	PLEXO	5	6	7	6,00
C-SRV	CALL CENTER - IKONO CC	7	10	10	9,00
C-SRV	CORREO - GOOGLE WORKSPACE	8	8	10	8,67
C-SRV	PAGINA WEB	2	8	5	5,00

Tabla 6. Valoración de los activos

Fuente. Elaboración propia

11.3 Evaluación de Amenazas (Escenario de Riesgos)

Para realizar la identificación del escenario de riesgos, se tuvieron en cuenta las amenazas determinadas en el catálogo de la norma ISO 27005:2011, dicho proceso se realizó teniendo en cuenta los activos de información previamente contemplados en la valoración de activos con una calificación mayor o igual 8, descuidos a continuación:

- HIS/ISalud,
- Plataforma Call Center,
- Correo Google-WorkSpace,
- Firewall (Asis),
- Servidor (Zeus)
- Firewall (Admin)

Los resultados obtenidos después de realizar la identificación del escenario de riesgos fueron los siguientes:

Activo	Nº Amenazas
HIS/ISalud	20
Call Center	17
Correo Google-WorkSpace	10
Firewall (Asis)	26
Servidor Zeus	27
Firewall (Admin)	26
TOTAL	126

Para más información revisar el anexo C

11.4 Análisis de Riesgos

Para realizar el análisis de riesgos se tuvieron en cuenta los activos de información asociados a sus respectivas amenazas identificados previamente en el escenario de riesgos; dicho análisis se realizó determinando la probabilidad y el impacto con los valores relacionados en la tabla 7 y 8 respectivamente, que tienen cada uno de esos activos con respecto a cada una de las amenazas; se obtuvo como resultado el nivel de riesgo asociado a cada activo mediante la fórmula:

Nivel de riesgo = Probabilidad x Impacto

Los valores de referencia se definieron de la siguiente manera:

TABLA PARA ESTIMAR LA PROBABILIDAD			
NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
5	Frecuente	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de una vez al año
4	Probable	El viable que el evento ocurra en la mayoría de las circunstancias.	Al menos una vez en el último año
3	Ocasional	El evento podría ocurrir en algún momento.	Al menos una vez en los últimos dos (2) años
2	Posible	El evento puede ocurrir en algún momento.	Al menos una vez en los últimos cinco (5) años
1	Improbable	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).	No se ha presentado en los últimos cinco (5) años

Tabla 7. Estimación la Probabilidad

Fuente. Elaboración propia

TABLA PARA ESTIMAR EL IMPACTO			
VALOR	CONSECUENCIA	DESCRIPCIÓN	
5	Catastrófico	Crítico, que existen importantes errores, severos incumplimientos en el marco regulatoria y afecta fuertemente el cumplimiento de los objetivos.	
4	Peligroso	Errores significativos continuos, existen incumplimientos a los puntos de control internos y algunas disposiciones legales.	
3	Moderado	Errores significativos ocasionales, existen incumplimientos a los puntos de control internos y algunas disposiciones legales.	
2	Menor	Errores operativos, existen incumplimientos en algunos puntos de control internos, pero no constituyen infracciones a la ley.	
1	Insignificante	Errores operativos, existen incumplimientos en algunos puntos de control internos, pero son subsanables inmediatamente.	

Tabla 8. Estimación del Impacto

Fuente. Elaboración propia

Los resultados obtenidos después de realizar el análisis de riesgos (probabilidad * impacto) fueron los siguientes:

17 riesgos con calificación 25,
6 riesgos con calificación 20,
6 riesgos con calificación 15,
3 riesgos con calificación 12,
9 riesgos con calificación 10,
2 riesgos con calificación 9,
8 riesgos con calificación 8,
20 riesgos con calificación 6,
10 riesgos con calificación 5,
5 riesgos con calificación 4,
6 riesgos con calificación 3,
8 riesgos con calificación 2 y 26 riesgos con calificación 1

En la tabla siguiente se puede observar el escenario de riesgo en las dimensiones probabilidad e impacto que dan como resultado el riesgo.

ANÁLISIS DE RIESGOS					
ESCENARIO DE RIESGO	PROBABILIDAD		IMPACTO		RIESGO
HIS / Isalud - La falta de equipo de telecomunicaciones (Canales Datos, MPLS, Internet)	Posible	2	Moderado	3	6
HIS / Isalud - La Manipulacion Software	Improbable	1	Catastrófico	5	5
HIS / Isalud - La saturación del sistema de información	Probable	4	Catastrófico	5	20
HIS / Isalud - Mal funcionamiento de software	Improbable	1	Menor	2	2
HIS / Isalud - El incumplimiento de la mantenibilidad del sistema de información	Posible	2	Peligroso	4	8
HIS / Isalud - La Corrupcion de los datos	Improbable	1	Peligroso	4	4
HIS / Isalud - Error en Uso	Posible	2	Moderado	3	6
HIS / Isalud - Ataques de identificación y autenticación de usuarios.	Posible	2	Moderado	3	6
HIS / Isalud - Inadecuada configuración de la aplicación y/o sistemas.	Improbable	1	Moderado	3	3
HIS / Isalud - Interrupción continua de sesiones de trabajo	Improbable	1	Menor	2	2

Tabla 9. Análisis de Riesgos

Fuente. Elaboración propia

La información descrita aquí está ampliada en el Anexo E de este documento

11.5 Matriz de Riesgos

La matriz de calor se obtiene después de realizar el análisis de riesgos, donde se ubica cada uno de los activos de información de acuerdo con su nivel de riesgo, distinguiéndolos por colores según el nivel de criticidad, los cuales traen consecuencias graves reseñables para la organización, especificando que el color rojo tiene un valor extremo, el color naranja un valor alto, el color amarillo un valor moderado y el color verde un valor bajo como se puede observar a continuación:

MAPA DE RIESGO

Probabilidad		Impacto				
	Valor	Insignificante	Menor	Moderado	Peligroso	Catastrofico
		1	2	3	4	5
Frecuente	5				R39 R46	R11, R13, R18. R44. R58, R66, R67, R68, R69. R85, R93, R97. R123, R131, R132, R133, R134.
Probable	4	R12				R3. R24. R73 . R138.
Ocasional	3	R31	R79. R117.	R20. R37.	R48. R74. R113.	R51, R65. R78, R92. R116, R130.
Posible	2		R53 R80 R118	R1, R7, R8, R15 R21, R23, R27, R28, R33 R38, R40 R50, R54 R76, R77, R81	R5, R16. R22, R26, R34. R49 R75 R114	R14, R17 R32, R35 R42 R45, R72, R100, R137
Improbable	1	R19, R36. R47. R52, R55, R61, R62 R63, R64, R70, R71. R82, R88, R89, R90 R91, R94, R98, R99. R120, R126, R127, R128 R129, R135, R136.	R4,R10. R25,R30. R41,R43. R95 R96.	R9 R29. R57. R84. F122.	R6	R2 R56, R59, R60 R83, R86, R87 R121, R124, R125

Figura 19. Mapa de riesgo

Se utilizó una matriz de 5x5 para el mapa de calor

Luego de darle valoración a los riesgos, se realiza la matriz de riesgo, donde se maneja probabilidad improbable, posible, ocasional y probable, frecuento por impacto insignificante, menor, moderado, peligroso y catastrófico.

ZONA	%	Total riesgos
DISTRIBUCIÒN PORCENTUAL		
ZONA	%	Total riesgos
Bajo	30,16%	38
Moderado	20,63%	26
Alta	16,67%	21
Extremo	32,54%	41
TOTAL	100,00%	126

Figura 20. Mapa de riesgo distribución porcentual de los riesgos

Fuente. Elaboración propia

Después de realizar la valoración de los riesgos aplicando los catálogos de vulnerabilidades y amenazas contenidos en la norma ISO 27005:2011, se identificaron un total de 126 riesgos en Calculaser, de los cuales 41 riesgos se encuentran en una zona Extremo con un porcentaje 32.54%, 21 riesgos en una zona Alta con un porcentaje de 16,67%, 26 riesgos en una zona Moderado con un porcentaje de 20,63% y 38 riesgos en una zona Bajo con un porcentaje de 30,16%.

11.6 Tratamiento de Riesgos

Después de tener identificados los niveles de riesgo para cada activo de información que, según el mapa de calor calificados con un nivel de riesgo extremo, son analizados en la matriz de riesgo, en donde para cada uno de ellos se seleccionan las amenazas, las vulnerabilidades para obtener los riesgos. Luego se evalúa el impacto para la organización en diferentes aspectos, siendo estos la confidencialidad, integridad y la disponibilidad, con unos valores para su medición entre bajo, moderado y alto. Seguido, se evalúa desde el punto de vista operativo, financiero, jurídico, de sanción o multas, de imagen reputacional, tecnológico y de medio ambiente con valores asignados de insignificante, menor, dañino, severo y crítico. Luego, se selecciona la estrategia que se le va dar al riesgo entre asumir, eliminar, mitigar y transferir para después seleccionar el control según el anexo A de la norma ISO 27001:2013 y el control de la norma ISO 27032:2012 y el tipo de control si es preventivo, correctivo o detectivo. Por último, se asigna el nombre del colaborador o cargo responsable, con el plazo en días o meses y la fecha de implementación.

De los 41 Riesgos identificados 38 se van a mitigar con la implementación de los controles y los 3 restantes se van a asumir por las condiciones actuales de las edificaciones.

Para ampliar la información revisar el anexo F.

11.6.1 Plan de Tratamiento de Riesgos

Una vez ejecutadas las etapas de análisis y valoración de riesgos, y con base en los resultados obtenidos en la determinación real de riesgos, es necesario tomar decisiones basado en los niveles de riesgo obtenidos.

Si el riesgo se ubica en una zona de riesgo no aceptable, cada líder responsable de los riesgos identificados debe implementar los controles definidos, se definen las posibles acciones que permiten gestionar los riesgos inaceptables en el marco de la seguridad de la información e implementar controles necesarios para proteger la misma.

A continuación, se nuestra la estrategia para abordar los riesgos y establecer su tratamiento.

PLAN DE TRATAMIENTO DE RIESGOS					
Descripción de actividades	Plan de Monitoreo	Recursos generales y financieros necesarios	Persona responsable	Plazos de inicio y finalización	Estado
Implementar un WAF (Firewall de Aplicaciones Web) que garantice la protección contra el OWASP Top 10	Configuración de reglas con notificaciones de comportamientos o evento como (SQL Injection, XSS etc)	$ 50.000.000	Gerente	180 días	Pendiente
Implementar una pasarela de correo electronico seguro que protega las herramientas colaborativas de malware, ataques 0 Day y motores de AntiSpam avanzandos con IA	Configuración de reglas con notificaciones de comportamientos anómalos (Malware, Spam, Phising, Zero Day, etc)	$ 10.000.000	Gerente	180 días	Pendiente
Implementar dispositivos de seguridad perimetral en esquemas de alta disponibilidad donde se garantice la continuidad del servicio, con funcionalidades de IDS, IPS con Anti DoS y DDoS, y con tecnologías de ZTNA	Configuración de reglas con notificaciones de comportamientos anómalos (Ataques DoS, Ddos)	$ 50.000.000	Gerente	180 días	Pendiente
Implementar servidores con tecnologías de protección redundante (energía, almacenamiento)	Configuración de notificaciones de las utilidades del servidor	$ 20.000.000	Gerente	180 días	Pendiente
Implementar sistemas de detección y extinción de incendios o extintores de Co2	Matener un monitoreo constante sobre las instalaciones	$ 15.000.000	Gerente	180 días	Pendiente
Implementar un procedimiento para la gestión de cambios de TI	Revisión periodica de los registro derivados de la gestion de cambios de TI	N/A	Gerente	180 días	Aprobación

Tabla 10. Plan de Tratamiento de Riesgos

Fuente. Elaboración propia

11.7 Arquitectura y Tecnologías Propuestas para Calculaser

11.7.1 Arquitectura

Después de analizar la matriz de riesgos y revisados los planes de acción técnicos descritos en el plan de tratamiento de riegos, y con el fin de minimizar las diferentes brechas de ciberseguridad en Calculaser SA, hemos trazado una hoja de ruta, como arquitectura general de ciberseguridad para la organización, la misma tiene los siguientes elementos:

- Seguridad perimetral con NGFW con módulos de IPS y IDS de última generación en todas las sedes, incorporación de tecnologías de Sandboxing.
- Arquitectura basada en SD-WAN para redundancia de conexiones, continuidad de negocio y mejoramiento del rendimiento de los aplicativos.
- Multifactor de autenticación para conexiones remotas de los usuarios.
- VPNs site to site para la comunicación entre las diferentes sedes de la compañía y proveedores.
- VPNs client to site SSL para acceso remoto hacia los recursos informáticos, con MFA2.
- Endpoint y EDR de última generación para la protección de los equipos de punto final.
- Ciberseguridad de correo electrónico, para mitigar una de las brechas principales en seguridad, basado en IA
- Portal unificado de administración de la solución.

- Logs consolidados y análisis forense integrado para trazabilidad de posibles problemas.
- Seguridad basada en WAF y protección de APIs corporativas, para el aseguramiento de las aplicaciones WEB críticas, como su HIS/ISalud y la plataforma de gestión del call center y como opcional proteger ERP Yeminus

11.7.1.1 Arquitectura Detallada y Documentada

La arquitectura consolidada se puede ver en la figura 20 y se detalla en este capítulo

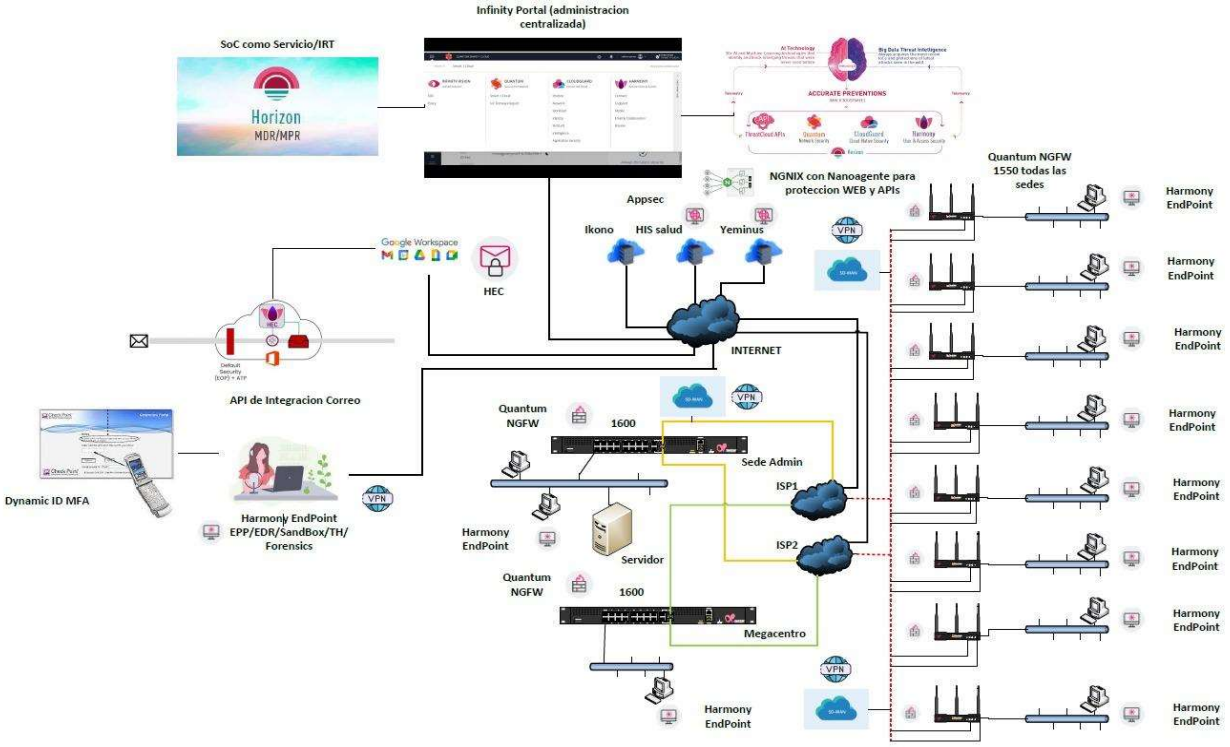


Figura 21. Arquitectura propuesta

11.7.1.1.1 Arquitectura Detallada de NGFW

Firewalls principales, sedes Administrativa y Megacentro (ver figura 22)

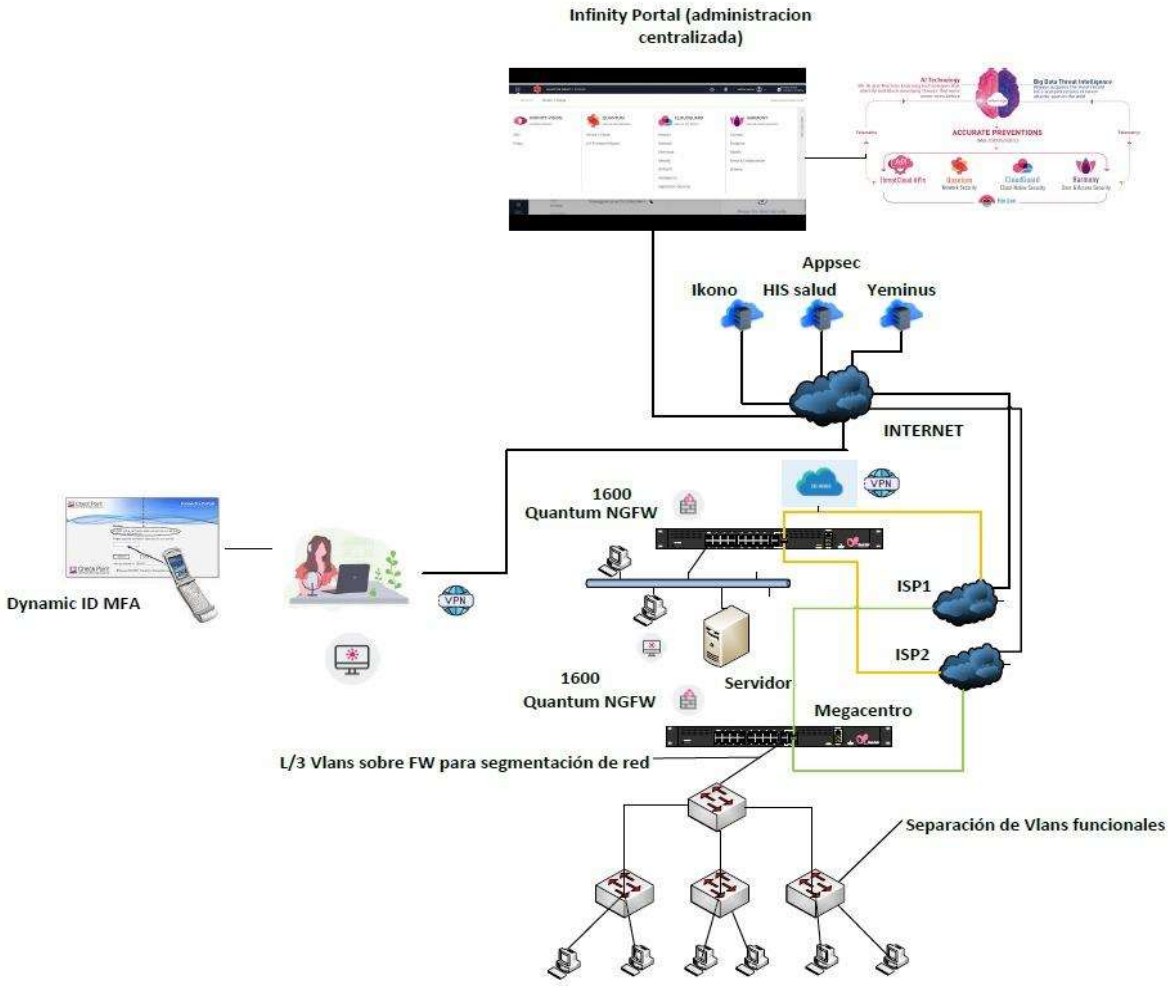


Figura 22. Arquitectura Next Generation Firewall

El esquema de conectividad consta de unos Quantum 1600 en cada una de las sedes mencionadas, con licencia SNBT (sandblast, lo cual es la más efectiva para contrarrestar los ataques de V generación que veremos numeral 11.7.2 en párrafos posteriores, la misma contiene lo siguiente:

Security Technologies for Gateways

Technology	NGFW	NGTP	SandBlast
Firewall	✓	✓	✓
VPN (IPsec)	✓	✓	✓
IPS	✓	✓	✓
Application Control	✓	✓	✓
Content Awareness	✓	✓	✓
URL Filtering		✓	✓
Anti-bot		✓	✓
Anti-Virus		✓	✓
Anti-Spam		✓	✓
SandBlast Threat Emulation			✓
SandBlast Threat Extraction			✓

Figura 23. Tecnologías de seguridad para gateways

Cada uno de estos Firewall tendrá un esquema de conexión basado en SD-WAN, enlaces verdes y amarillos, con 2 proveedores de servicio, el sistema podrá analizar dinámicamente la latencia, perdida y jitter de los enlaces.

En los diferentes aplicativos que se pueden detectar con los Firewall, generando políticas de balanceo dinámico, fail over y mejor path de conexión, para así tener el máximo rendimiento en la WAN corporativa (ver figura 23)

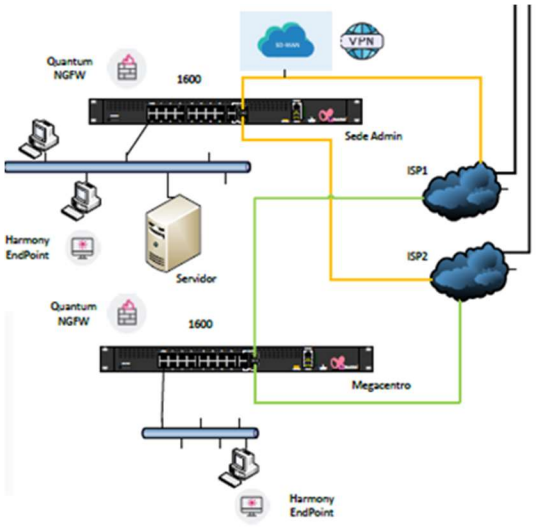


Figura 24. Enlaces redundantes con los ISP

11.7.1.1.2 Mejoramiento de perímetro

Un cortafuego es una parte necesaria de cualquier arquitectura de seguridad y elimina las conjeturas sobre las protecciones a nivel de host y las confía a su dispositivo de seguridad de red.

En una red debidamente segmentada, los cortafuegos imponen el acceso mínimo privilegiado de confianza cero para dispositivos, usuarios, grupos, aplicaciones se implantará en Calculaser.

Esto incluye controles fronterizos de macro-segmentación para el tráfico norte/sur que entra y sale del segmento protegido y micro-segmentación para inspeccionar el tráfico que entra y sale del segmento protegido entre máquinas virtuales y/o servidores.

Los cortafuegos también son dispositivos de red polivalentes. Utilizan. Traducen las direcciones de red de una red a otra, de privada a pública y de IPv4 a IPv6. Son puntos de terminación de redes privadas virtuales (VPN) para VPN de sitio a sitio y de cliente a sitio.

Cuando el trabajo pasó a ser remoto a principios de 2020, las capacidades de acceso remoto VPN y portal SSL VPN fueron vitales para mantener a los empleados conectados. Quizá la más importante de todas estas funciones sea la prevención de amenazas.

Los cortafuegos de nueva generación se centran en bloquear el malware y los ataques a la capa de aplicación. El IPS (sistema de prevención de intrusiones) integrado en los cortafuegos de nueva generación permite a las empresas parchear virtualmente los sistemas vulnerables, a veces antes de que se desarrolle una actualización de seguridad.

La prevención es la clave. Toda red necesita una defensa contra el malware, y una defensa avanzada implica muchas capas de protección. Hay muchos tipos de malware contra los que un cortafuego puede proteger, entre los que se incluyen:

- Virus
- Gusanos
- Troyanos
- Programas espía
- Adware
- Phishing
- Ransomware

También hay que señalar que los cortafuegos son omnipresentes en los regímenes de cumplimiento normativo. Suelen ser suelen ser obligatorios para proteger los sistemas de la organización de Internet y de otras partes del entorno de la organización, están configurados con políticas de seguridad que deniegan todo el tráfico excepto el necesario para las aplicaciones de producción, protegen los datos en tránsito dentro de túneles cifrados y también pueden aplicar los controles de prevención de amenazas necesarios para cumplir la normativa.

11.7.1.1.3 Casos de uso a instalar en Calculaser

- Control de acceso: El control de acceso define las personas o grupos y los dispositivos que tienen acceso a las aplicaciones y sistemas de red, denegando así el acceso no autorizado y, tal vez, las amenazas.

- VPN de acceso remoto: La VPN de acceso remoto proporciona acceso remoto (ver figura 24 acceso VPN) y seguro a la red de una empresa a hosts o clientes individuales, como teletrabajadores, usuarios móviles y consumidores de extranet. Cada host suele disponer de un software cliente VPN o utiliza un cliente basado en web. La privacidad y la integridad de la información confidencial se garantizan mediante la autenticación multifactor, el escaneado de conformidad de los terminales y el cifrado de todos los datos transmitidos.

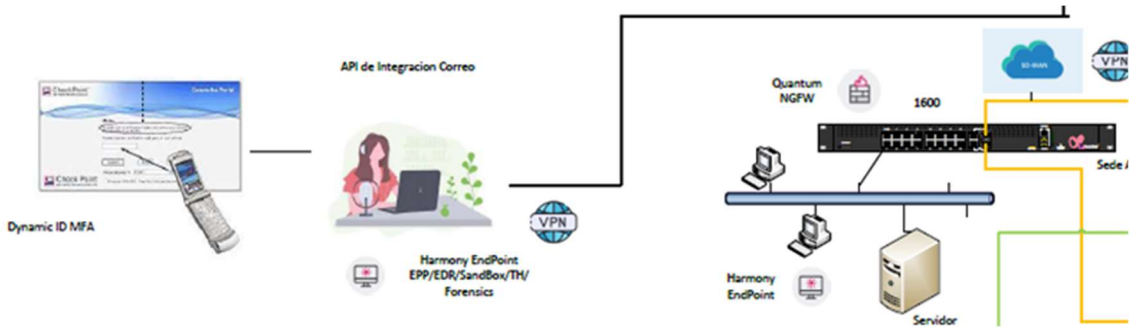


Figura 25. Acceso VPN.

Desde el endpoint que exploremos más adelante se tendrá capacidad total de VPN, con administración centralizada desde un portal único y MFA2 bajo un sistema SMS en mensajes de texto al celular, integrado por cualquier carrier del mercado colombiano.

- Redes de confianza cero: El modelo de seguridad de confianza cero establece que un usuario sólo debe tener el acceso y los permisos que necesita para desempeñar su función. Se trata de un enfoque muy diferente del que ofrece el modelo de seguridad tradicional centrado en el perímetro.

La confianza cero es un enfoque de seguridad mediante la micro-segmentación. Utilizando cortafuegos, las empresas pueden aplicar una política de acceso con mínimos privilegios a nivel de red. Así, sólo los usuarios y dispositivos adecuados tienen el acceso que necesitan para desempeñar sus funciones. (ver figura 26)

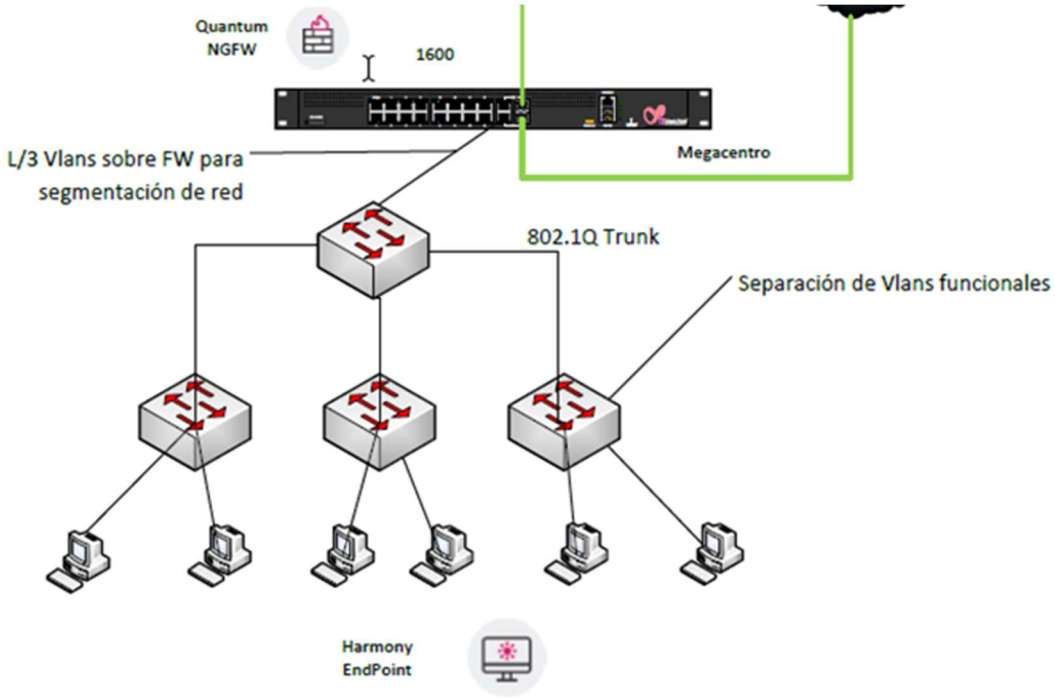


Figura 26. Redes de confianza cero

• Seguridad en la Web: La Web es tan omnipresente que requiere capacidades de inspección de protocolos web en constante actualización, categorizar con precisión millones de sitios web, objetos dinámicos para actualizar automáticamente las listas de sitios de confianza.

Las amenazas utilizan las infraestructuras web para ocultar actividades maliciosas y explotar directa o indirectamente las vulnerabilidades de los usuarios, engañandolos con campañas de phishing.

- Sistemas de prevención de intrusiones - IPS: Las tecnologías IPS pueden detectar o prevenir ataques a la seguridad de la red, como los de fuerza bruta, los de denegación de servicio (DoS) y los que aprovechan vulnerabilidades conocidas. Una vulnerabilidad es un punto débil, por ejemplo, en un sistema un exploit es un ataque que aprovecha esa vulnerabilidad para hacerse con el control de ese sistema.

Cuando se anuncia un exploit, suele haber una ventana de oportunidad para que los atacantes aprovechen esta vulnerabilidad antes de que se aplique el parche de seguridad. En estos casos puede utilizarse un sistema de prevención de intrusiones para bloquear rápidamente estos ataques.

- Sandboxing: Sandboxing es una práctica de ciberseguridad en la que se ejecuta código o se abren archivos en un entorno seguro y aislado, usando una máquina anfitriona que imita los entornos operativos del usuario final. Sandboxing observa los archivos o el código a medida que se abren y buscan comportamientos maliciosos para evitar que las amenazas entren en la red.

Por ejemplo, el malware de archivos PDF, Microsoft Word, Excel y PowerPoint puede detectarse y bloquearse de forma segura antes de que lleguen a un usuario final desprevenido.

- Control de aplicaciones: El control de aplicaciones en un firewall de nueva generación se refiere a la capacidad de un firewall para identificar y controlar el tráfico de aplicaciones específicas en una red.

A diferencia de los firewalls tradicionales que solo pueden controlar el tráfico por dirección IP y puerto, un firewall de nueva generación utiliza tecnologías más avanzadas para analizar el tráfico y determinar qué aplicación lo está generando.

Para lograr esto, un firewall de nueva generación utiliza técnicas como la inspección profunda de paquetes, la identificación de aplicaciones mediante la comparación de patrones de tráfico y la utilización de bases de datos de firmas de aplicaciones conocidas.

Una vez que se identifica la aplicación que está generando el tráfico, el firewall puede aplicar políticas de seguridad específicas a esa aplicación, como bloquear, permitir o limitar su uso.

El control de aplicaciones en un firewall de nueva generación es importante porque muchas aplicaciones en línea pueden representar una amenaza para la seguridad de una red, como aplicaciones de intercambio de archivos peer-to-peer, aplicaciones de mensajería instantánea o redes sociales.

Al identificar y controlar el tráfico de estas aplicaciones, los firewalls de nueva generación pueden ayudar a proteger una red contra amenazas cibernéticas.

SD-WAN como modelo de conectividad para Calculaser

SD-WAN es el acrónimo de Software-Defined Wide Area Network, que significa "Red de Área Amplia Definida por Software". Es una tecnología que permite la optimización y gestión inteligente de las redes de área amplia, proporcionando una solución de conectividad más flexible, rentable y segura para las empresas.

En una red tradicional de área amplia (WAN), los routers y otros dispositivos de red se configuran manualmente para establecer conexiones de red. Con SD-WAN, los dispositivos de red se gestionan de manera centralizada mediante software, lo que permite a los administradores de red definir las políticas de red y la asignación de ancho de banda para cada aplicación, permitiendo una mayor flexibilidad y control en la administración de la red.

Además, SD-WAN utiliza técnicas de enrutamiento inteligente para optimizar el tráfico de red, lo que permite una mejor utilización de los recursos de red y mejora la calidad de la conexión de red. También puede reducir los costos de ancho de banda y simplificar la implementación y la gestión de la red, lo que resulta en una solución de conectividad más rentable para las empresas.

Para Calculaser SD-WAN es una tecnología de red que permite una gestión más eficiente, flexible y rentable de las redes de área amplia, proporcionando una solución de conectividad segura y de alto rendimiento (ver Figura 27)

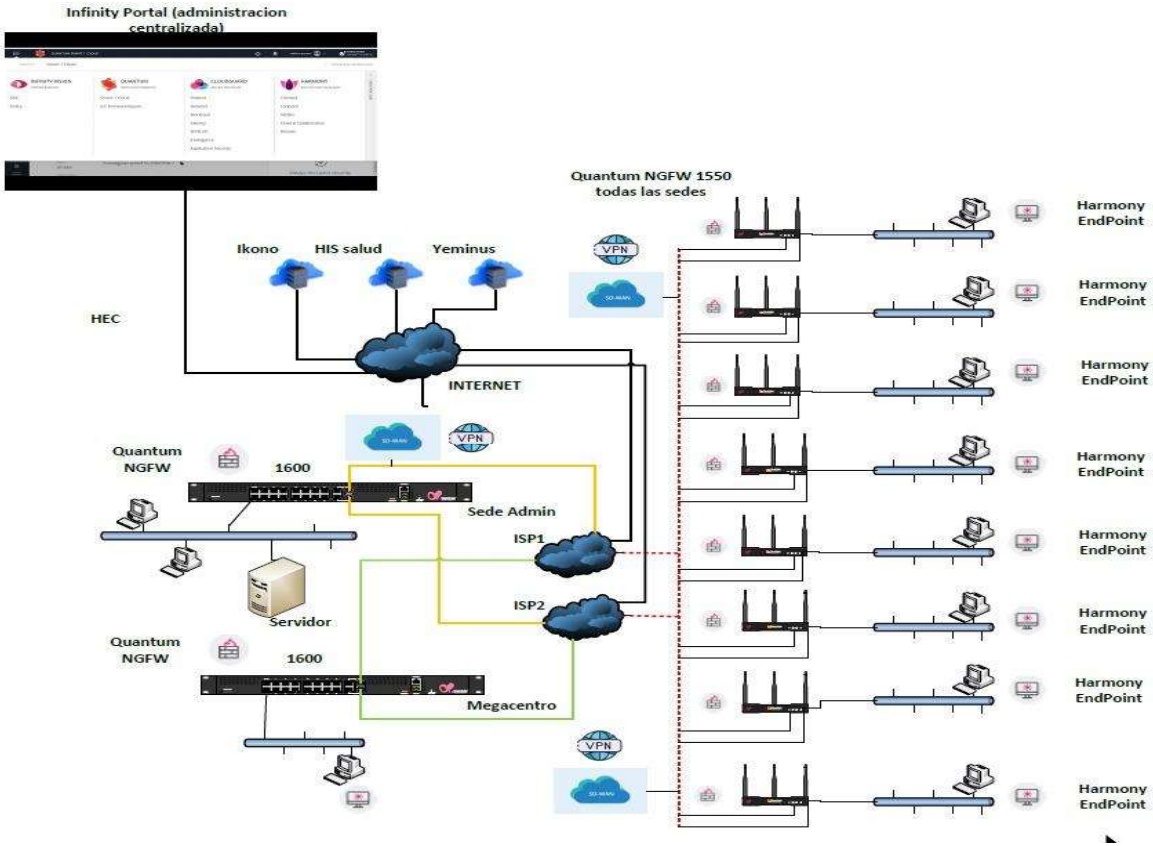


Figura 27. Tecnología SD-WAN

En este caso cada sede poseerá 2 canales a internet para redundancia y balanceo de los canales, logrando identificar de manera inteligente el jitter, la latencia y la pérdida de cada enlace, para encontrar el mejor path hacia la aplicación, sea en premisa usando las VPNs punto a punto y los servicios SAAs como Yeminus o HIS Salud, aumentado dramáticamente el rendimiento de la WAN y asegurando la continuidad del negocio en caso de falla de algún carrier.

Todo el sistema SD-WAN estará controlado por un dashboard central basado en nube

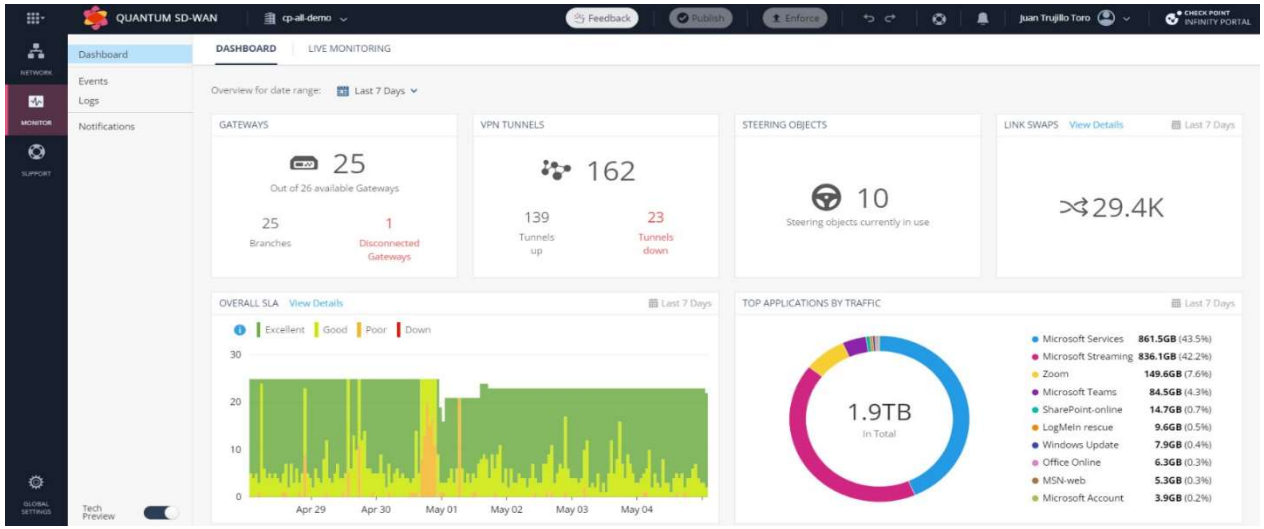


Figura 28. Dashboard para tecnología SD-WAN

11.7.1.1.4 Seguridad IoT

La seguridad IoT (Internet de las cosas) es un conjunto de prácticas y medidas de seguridad diseñadas para proteger los dispositivos IoT y las redes que los conectan de los riesgos de seguridad cibernética. Los dispositivos IoT incluyen cualquier dispositivo conectado a Internet que pueda recopilar y transmitir datos, como sensores, cámaras, altavoces inteligentes, termostatos, cerraduras y muchos otros.

Dado que los dispositivos IoT recopilan y transmiten datos como los dispositivos médicos de Calculaser, la seguridad de estos dispositivos es crítica para proteger la privacidad y la seguridad de los datos transmitidos.

Algunas de las principales amenazas de seguridad en los dispositivos IoT incluyen el acceso no autorizado, la manipulación de datos, la interceptación de datos y la inyección de código malicioso.

Los dispositivos IoT también pueden ser vulnerables a ataques de denegación de servicio (DoS) y ataques de ransomware.

El modelo de ciberseguridad para IoT (Internet de las cosas) para Calculaser incluye varios componentes clave, que se describen a continuación:

- Identificación: El primer paso en el modelo de ciberseguridad para IoT es identificar los dispositivos IoT y las redes que los conectan. Esto incluye la identificación de todos los dispositivos IoT en la red, así como el monitoreo de la actividad de la red para detectar posibles amenazas, esto se logra con el módulo de identificación de dispositivos IoT que viene incorporado en los FW perimetrales.

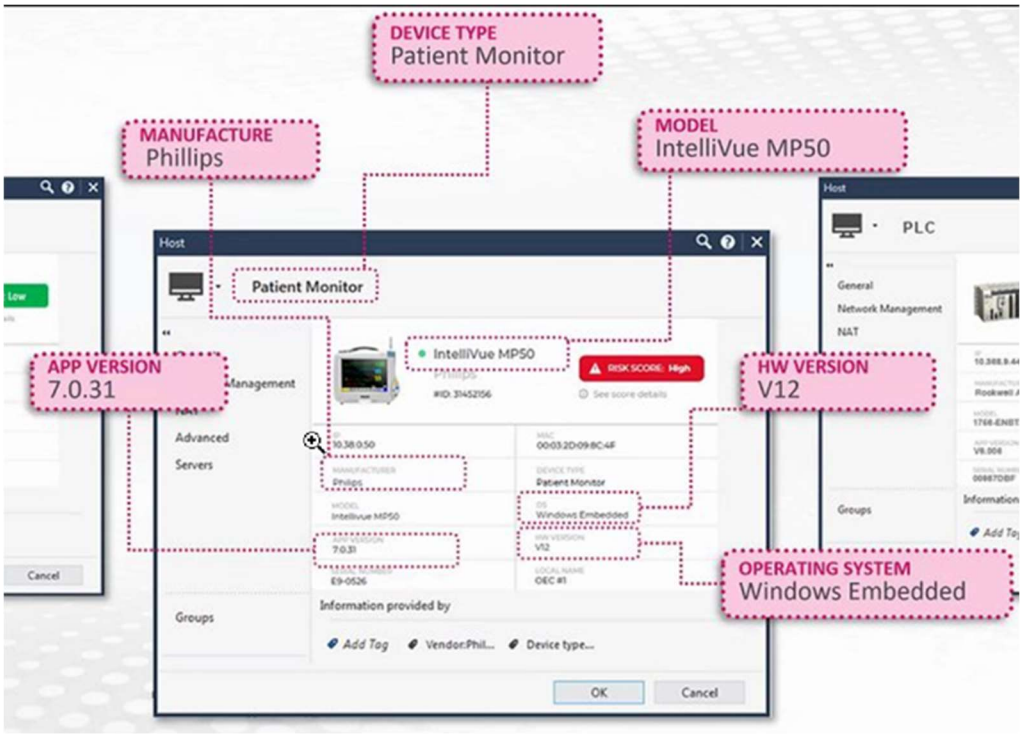


Figura 29. Módulo de identificación de dispositivos IoT

- Protección: La protección es el segundo componente clave del modelo de ciberseguridad para IoT. Esto implica la implementación de medidas de seguridad adecuadas para proteger los dispositivos IoT y las redes que los conectan contra posibles amenazas.

Las medidas de seguridad pueden incluir la autenticación y autorización adecuadas, el cifrado de datos, el monitoreo de la actividad de la red y la implementación de parches de seguridad.

- Detección: La detección es el tercer componente clave del modelo de ciberseguridad para IoT. Esto implica la detección temprana de posibles amenazas y vulnerabilidades en los dispositivos IoT y la red. Esto puede incluir la implementación de sistemas de monitoreo y análisis de amenazas en tiempo real.

El modelo de arquitectura de red para lograr este nivel de protección se logra mediante la incorporación de una Vlan específica en los SWs de Calculaser s.a, para todos los dispositivos IoT y otra para los equipos médicos, aquí se colocaran las capacidades de detección de dispositivos IoT en los FW y se crearán las políticas de seguridad automatizadas, dependiente de su hardware, además se aplicará el sistema IPS de los FWs para lograr parchado virtual en estas redes, blindándolas contra explotación de vulnerabilidades.

Este modelo como se ha mencionado requiere la segmentación de tráfico de estas vlans tanto norte-sur como este-oeste (ver figura 30)

Figura 30. Segmentación de la red en VLANs

En los SWs de Calculaser se crearán las VLANs para cada zona de seguridad, donde el terminador a nivel de L/3 será el dispositivo NGFW con módulo de IoT (ver figura 31)

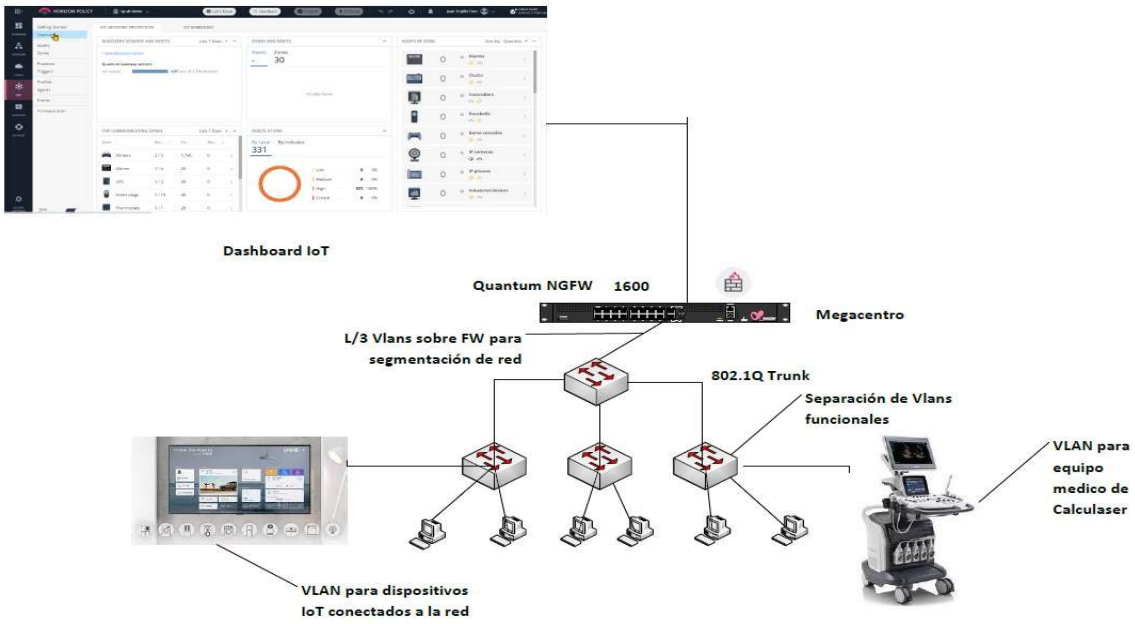


Figura 31. Segmentación de la Red VLANs desde el NFGW

Luego de esto aplicaremos parchado virtual sobre el módulo de IPS

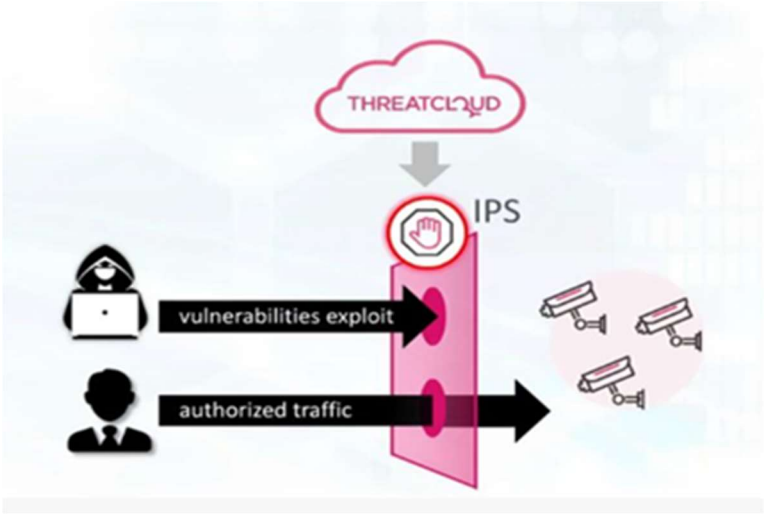


Figura 32. Parchado de aplicaciones a los IPS

11.7.1.1.5 Solución de EndPoint

Si analizamos la arquitectura de seguridad para Calculaser, uno de los puntos más importante es la incorporación de un agente de endpoint, con capacidades avanzadas de detección de malware, EDR y Sandboxing, como última línea de defensa, hacia todos los problemas de ciberseguridad que hemos discutido.

El Endpoint es una solución de seguridad diseñada para proteger los dispositivos finales y los servidores en las redes empresariales contra amenazas avanzadas, como malware, phishing, ransomware y otros tipos de ataques cibernéticos.

¿Cómo funciona el endpoint en Calculaser S.A.?

Funciona mediante la instalación de un agente de seguridad en cada dispositivo final y servidor en la red empresarial. Este agente de seguridad se comunica con un servidor de gestión centralizado que monitorea la actividad de los dispositivos finales y los servidores en tiempo real.

El servidor de gestión también recibe actualizaciones de seguridad regulares para garantizar que la solución esté actualizada con las últimas amenazas cibernéticas.

Si se analiza la arquitectura, en cada punto final se instalará el agente, el cual sube a ser comandado por una nube de administración centralizada, la cual es la misma para toda la arquitectura de seguridad de la empresa

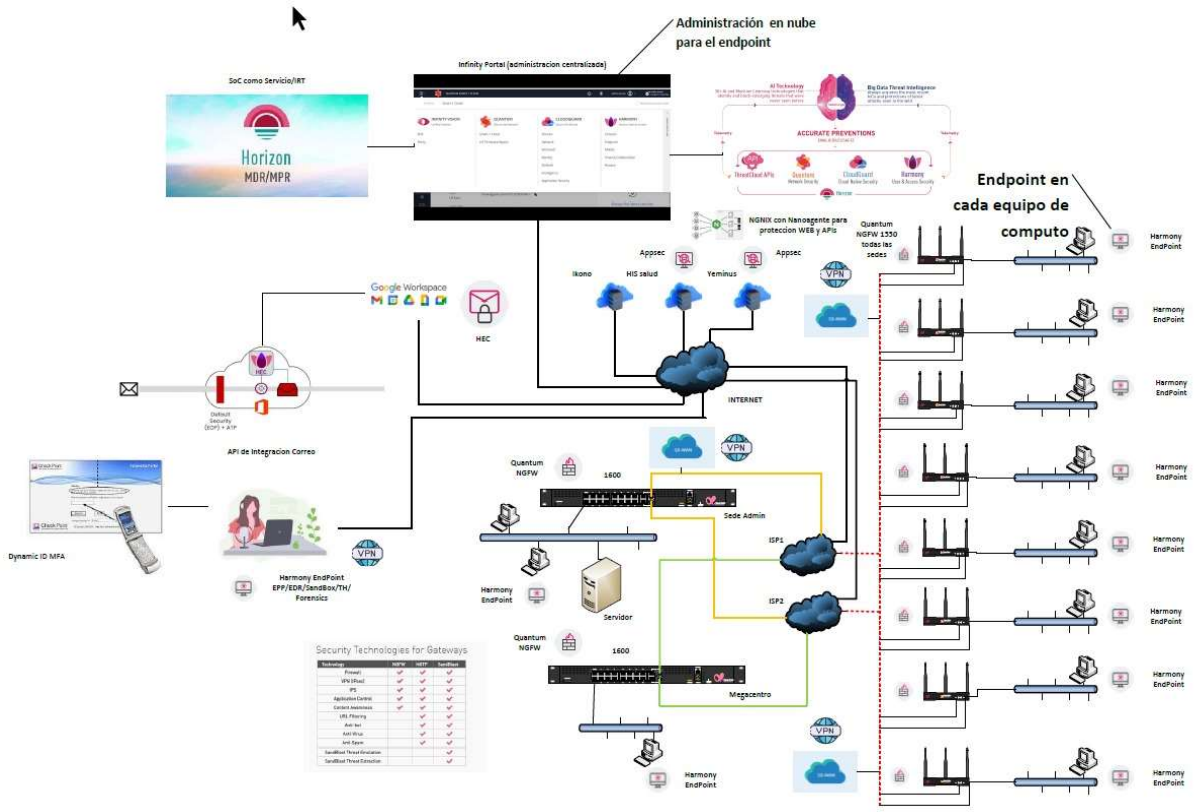


Figura 33. Solución EndPoint

Funciones específicas para Calculaser:

- Detección de amenazas avanzada: el agente utiliza tecnologías avanzadas de seguridad, como el aprendizaje automático y el análisis de comportamiento, para detectar amenazas que no se pueden detectar mediante firmas de virus tradicionales.

El aprendizaje automático es una técnica que utiliza algoritmos para analizar grandes conjuntos de datos y detectar patrones.

El mismo utiliza esta técnica para analizar el comportamiento de los archivos y los procesos del sistema en los dispositivos finales y los servidores. Si se detecta un

comportamiento anómalo, puede bloquear el archivo o el proceso y notificar al administrador de la red.

- Prevención de amenazas avanzada: el agente utiliza tecnologías de prevención de exploits para bloquear ataques de día cero y proteger los dispositivos finales y los servidores contra vulnerabilidades conocidas y desconocidas.

La prevención de exploits es una técnica que se utiliza para bloquear los ataques que aprovechan las vulnerabilidades de los sistemas.

Además, se utiliza esta técnica para bloquear los ataques de día cero, que son ataques que se aprovechan de vulnerabilidades desconocidas en los sistemas.

El agente también proporciona protección contra las vulnerabilidades conocidas, mediante la instalación de parches y actualizaciones de seguridad.

- Control de aplicaciones: el agente utiliza el control de aplicaciones para restringir el acceso a aplicaciones no autorizadas y evitar la filtración de datos confidenciales. El control de aplicaciones es una técnica que se utiliza para controlar el acceso a las aplicaciones en los sistemas.

El mismo utiliza esta técnica para restringir el acceso a las aplicaciones no autorizadas y garantizar que solo las aplicaciones autorizadas puedan acceder a los datos confidenciales.

Además, puede bloquear las aplicaciones que no cumplen con las políticas de seguridad de la empresa.

- Prevención de pérdida de datos (DLP): el agente utiliza la prevención de pérdida de datos (DLP) para monitorear y prevenir la filtración de datos confidenciales.

Si se está transfiriendo información confidencial fuera de la red de la empresa, el agente puede bloquear la transferencia y notificar al administrador de la red.

- Gestión de vulnerabilidades: el agente proporciona una gestión de vulnerabilidades avanzada para identificar y remediar las vulnerabilidades de seguridad en los dispositivos finales y los servidores.

Otro componente fundamental en la arquitectura de seguridad para Calculaser es el EDR dentro del mismo agente de protección

Endpoint Detection and Response (EDR) es una tecnología de seguridad que se utiliza para proteger los dispositivos finales en una red empresarial. EDR se centra en la detección y respuesta de amenazas avanzadas que pueden haber eludido las soluciones de seguridad tradicionales.

La tecnología EDR permite a los equipos de seguridad detectar amenazas en tiempo real, investigar y responder a las amenazas, y también proporciona informes detallados sobre la actividad maliciosa en los dispositivos finales.

El proceso de EDR se puede resumir en los siguientes pasos:

- Monitoreo continuo: EDR utiliza un monitoreo continuo para detectar cualquier actividad maliciosa en los dispositivos finales. Los sensores EDR se instalan en los dispositivos finales y recopilan información sobre la actividad en el sistema operativo, la actividad de la red, el comportamiento de los procesos y otros indicadores de compromiso (IOC).

- Análisis de comportamiento: Los datos recopilados por los sensores EDR se analizan para identificar patrones de comportamiento sospechosos. Los algoritmos de aprendizaje automático se utilizan para identificar amenazas conocidas y desconocidas mediante la comparación de la actividad observada con los patrones de actividad maliciosa conocidos.

- Alertas y respuestas: Si se detecta actividad maliciosa, el sistema EDR emite una alerta para que el equipo de seguridad pueda responder inmediatamente. Las alertas de EDR proporcionan información detallada sobre la actividad maliciosa, como la ubicación del dispositivo afectado, la gravedad de la amenaza y el tipo de amenaza.

- Investigación y remedio: Los equipos de seguridad pueden usar las alertas de EDR para iniciar una investigación detallada de la amenaza. La tecnología EDR también proporciona herramientas de respuesta automatizadas que permiten a los equipos de seguridad remediar las amenazas de manera rápida y efectiva.

- Análisis forense: EDR también se utiliza para la investigación forense después de un incidente de seguridad. La tecnología EDR proporciona informes detallados sobre la actividad maliciosa, lo que permite a los equipos de seguridad comprender mejor la naturaleza y el alcance del incidente y tomar medidas para prevenir incidentes futuros.

Lo que queremos lograr en Calculaser es contar con Endpoint Detection and Response (EDR) como tecnología de seguridad que se utilizará para proteger los dispositivos finales en una red empresarial.

11.7.1.1.6 Sandboxing como tecnología de protección para Calculaser en punto final:

Sandboxing es una técnica de seguridad que se utiliza para proteger los sistemas informáticos contra software malicioso y amenazas de seguridad avanzadas. El término se refiere a la creación de un entorno aislado en el que se puede ejecutar un programa o proceso sin que afecte al sistema operativo o a otros programas en ejecución en el sistema, esto lo logramos en el mismo agente de protección para Calculaser.

En la práctica, sandboxing se utiliza en varias áreas de la seguridad informática, incluyendo la protección contra malware, la investigación de amenazas, la depuración de software y la virtualización de sistemas.

El objetivo principal de sandboxing es proporcionar un entorno seguro y controlado en el que los programas o procesos puedan ejecutarse sin poner en peligro el sistema en su conjunto.

Para lograr esto, los entornos de sandboxing a menudo implementan medidas de seguridad adicionales, como limitar el acceso a recursos del sistema, monitorear la actividad del programa en ejecución y controlar el acceso a la red.

En la protección contra malware, sandboxing se utiliza para detectar y analizar programas maliciosos. El malware se ejecuta en un entorno de sandbox aislado y se observa su comportamiento. Si se detecta actividad maliciosa, se puede tomar acción de forma automática para bloquear la amenaza o informar a los usuarios y equipos de seguridad para su análisis.

El sandboxing también se utiliza en la investigación de amenazas, ya que permite a los analistas de seguridad observar el comportamiento de un programa malicioso sin poner en peligro el sistema.

Esto es especialmente útil para el análisis de amenazas avanzadas que pueden utilizar técnicas de evasión para evitar la detección de la seguridad tradicional.

En la depuración de software, el sandboxing se utiliza para aislar y solucionar problemas en el software sin afectar al sistema operativo o a otros programas en ejecución.

Esto es útil para el desarrollo de software y las pruebas de calidad, ya que permite a los desarrolladores trabajar de manera segura y sin afectar a otros usuarios o sistemas.

Finalmente, el sandboxing también se utiliza para la virtualización de sistemas, ya que proporciona un entorno aislado y seguro para la ejecución de aplicaciones o sistemas operativos.

Esto se utiliza comúnmente en entornos de desarrollo y prueba, donde los desarrolladores pueden probar su software en un entorno aislado y sin afectar a otros sistemas.

Este servicio de sandboxing se ejecutará en nube desde el agente de protección, enviando los archivos para su análisis y usando solo una consola de administración centralizada.

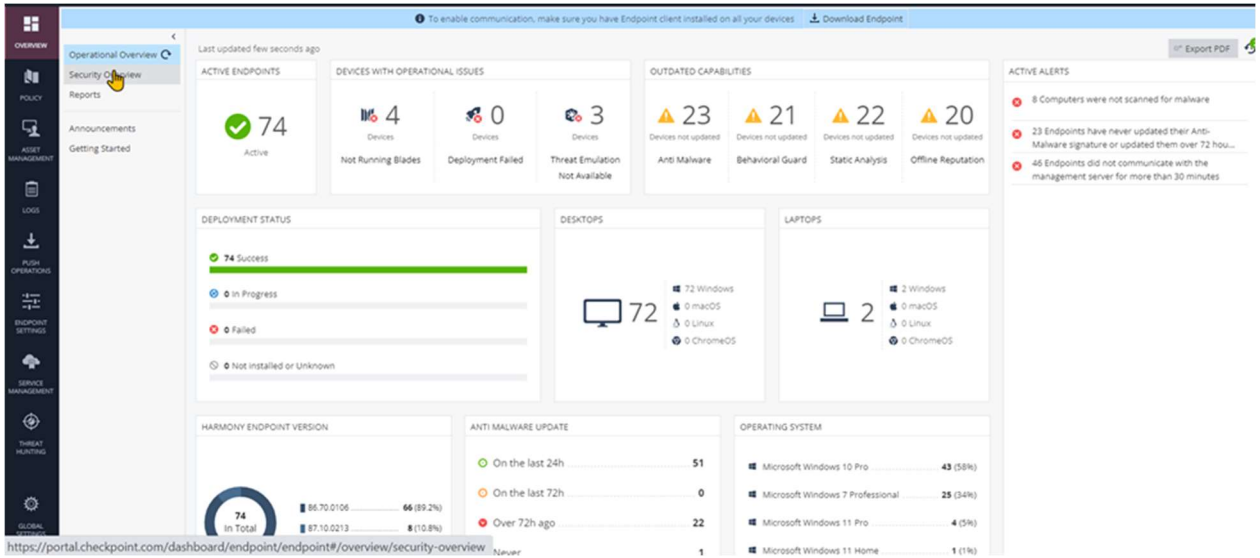


Figura 34. Visualización del EndPoint

11.7.1.1.7 Seguridad para correo electrónico basado en API de integración

La seguridad del correo electrónico es importante por varias razones, ya que el correo electrónico es una de las formas de comunicación más utilizadas en todo el mundo, tanto para uso personal como empresarial.

A continuación, se presentan algunas de las razones por las cuales la seguridad del correo electrónico es importante:

- Protección contra el correo no deseado (SPAM): Los correos no deseados pueden ser molestos y pueden contener virus y malware. Un filtro de correo electrónico puede ayudar a reducir la cantidad de correo no deseado que llega a la bandeja de entrada del usuario, y a su vez, reducir la posibilidad de que se abran archivos maliciosos.

- Protección contra el phishing: Los ataques de phishing son una forma común de fraude en línea en la que los atacantes envían correos electrónicos falsos que parecen legítimos, y que buscan engañar a los destinatarios para que proporcionen información confidencial como contraseñas o números de tarjeta de crédito. La seguridad del correo electrónico puede ayudar a detectar y bloquear los correos electrónicos de phishing antes de que lleguen a los destinatarios.

- Protección contra malware: Los correos electrónicos pueden contener archivos adjuntos maliciosos que pueden infectar el sistema del destinatario con malware. La seguridad del correo electrónico puede incluir herramientas que escanean y filtran los archivos adjuntos para detectar y bloquear malware.

- Cumplimiento normativo: Las empresas están sujetas a diversas regulaciones y leyes que requieren que ciertos tipos de información, como la información financiera y personal, sean protegidos y mantenidos confidenciales. La seguridad del correo electrónico puede ayudar a garantizar el cumplimiento normativo y proteger la información confidencial.

- Protección de la reputación: La seguridad del correo electrónico también puede ayudar a proteger la reputación de una empresa. Si una empresa es víctima de un ataque de phishing, por ejemplo, la reputación de la empresa podría verse comprometida si los clientes o socios comerciales se ven afectados.

- Protección de la privacidad: Los correos electrónicos a menudo contienen información personal y privada que debe ser protegida. La seguridad del correo electrónico puede ayudar a garantizar que los correos electrónicos sean encriptados y protegidos de manera adecuada para proteger la privacidad de los usuarios.

Integración Vía API

Para Calculaser la integración se logrará mediante API directa en Workspaces, lo que implica el no cambio de registros MX, reduciendo la complejidad de la instalación y latencia de los mismos al no pasar por un salto adicional, si observamos la arquitectura se muestra lo siguiente:

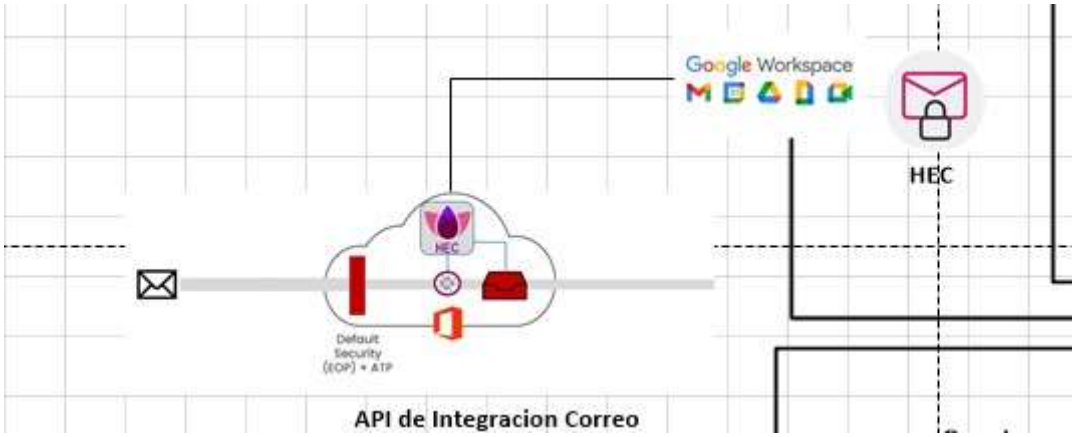


Figura 35. Integración Vía API

Como lo muestra la figura 35, el correo entrará directamente y el sistema de nativo de nube aplicará los primeros filtros, pasado los mensajes a la API de integración para ser analizados y filtrados, luego de esto se entregará el correo sin problemas a las bandejas de entrada de los usuarios, esto se ve en más detalle en la figura 36

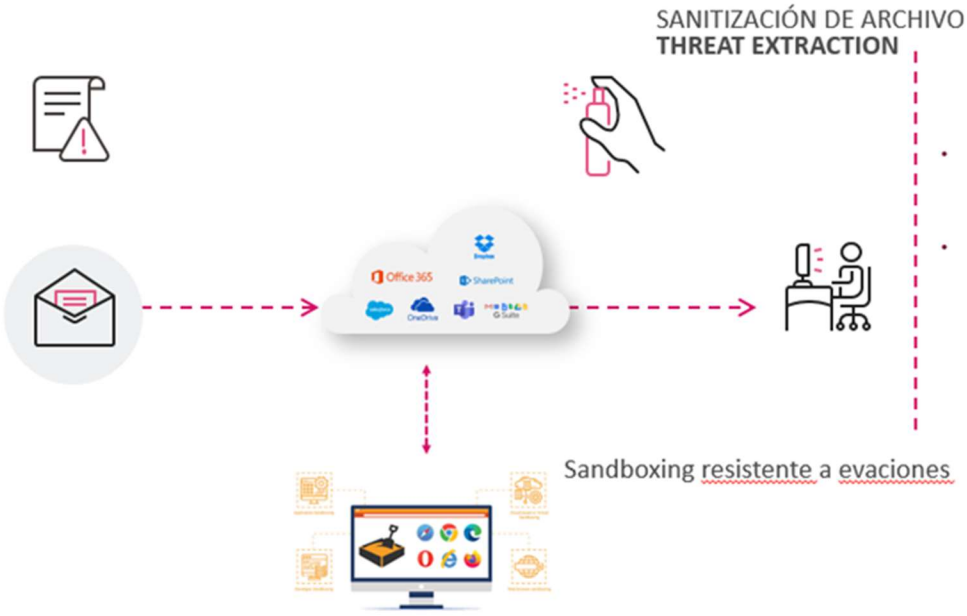


Figura 36. Entrega de correo

La solución de seguridad de correo electrónico y colaboración para Calculaser, proporciona una protección avanzada contra amenazas de correo electrónico.

La tecnología de seguridad avanzada, incluye la inteligencia artificial y el aprendizaje automático, para proteger contra amenazas conocidas y desconocidas. A continuación, se describen algunas de las características y beneficios principales para Calculaser:

- Protección contra amenazas avanzadas: utiliza múltiples capas de seguridad para proteger a las organizaciones contra amenazas avanzadas de correo electrónico, como phishing, spam, malware y virus. La solución utiliza tecnología de detección avanzada para identificar y bloquear amenazas antes de que lleguen a los usuarios finales.

- Análisis de amenazas en tiempo real: utiliza análisis de amenazas en tiempo real para detectar y bloquear nuevas amenazas de correo electrónico a medida que surgen. La solución analiza continuamente los patrones de comportamiento y las tendencias de las amenazas para mantenerse al día con las últimas amenazas de seguridad.

- Detección de amenazas avanzadas: utiliza técnicas avanzadas de detección de amenazas para identificar y bloquear amenazas que pueden pasar desapercibidas por otras soluciones de seguridad. La solución utiliza técnicas de aprendizaje automático y análisis de comportamiento para detectar patrones de amenazas y proteger a las organizaciones contra amenazas avanzadas.

- Gestión centralizada de políticas: se ofrece una gestión centralizada de políticas para garantizar que las políticas de seguridad se apliquen de manera coherente en toda la organización. Los administradores pueden configurar y administrar políticas de seguridad desde

una consola centralizada, lo que facilita la implementación de políticas de seguridad coherentes y efectivas.

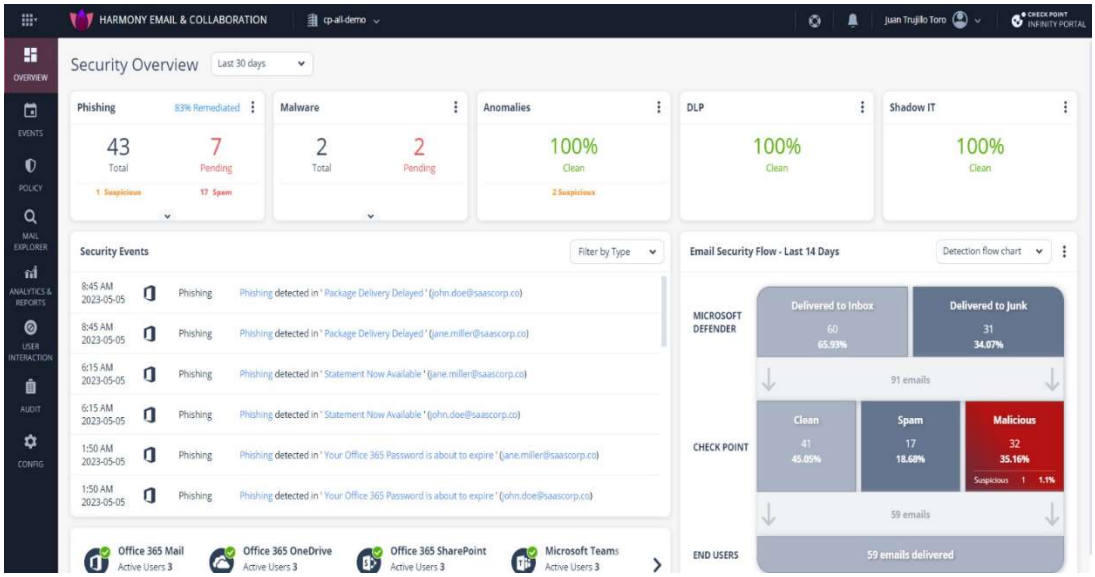


Figura 37. Interfaz de usuario

- Interfaz de usuario intuitiva: se cuenta con una interfaz de usuario (ver gráfica 14) intuitiva que permite a los usuarios navegar fácilmente por la solución y acceder a las funciones de seguridad. La interfaz de usuario simplifica la configuración y administración de políticas de seguridad, lo que permite a los administradores ahorrar tiempo y mejorar la eficiencia.

11.7.2 Arquitectura pensada para la protección contra ataques de V Generación.

Los ataques de quinta generación (también conocidos como ciberataques de próxima generación), son una nueva generación de ataques cibernéticos que utilizan técnicas avanzadas y automatizadas de inteligencia artificial (IA), aprendizaje automático para identificar y explotar vulnerabilidades en sistemas, y redes informáticas.

Estos ataques son muy sofisticados y pueden ser altamente efectivos, debido a la capacidad de la IA para adaptarse y evolucionar a medida que se enfrenta a nuevas defensas. Algunos ejemplos de técnicas utilizadas en estos ataques incluyen el uso de algoritmos de aprendizaje automático para identificar patrones en grandes conjuntos de datos, la utilización de sistemas de generación de lenguaje natural para engañar a los usuarios y la creación de malware que es capaz de evadir la detección por parte de los sistemas de seguridad.

Algunos ejemplos de ataques de quinta generación incluyen: el phishing avanzado, el spear phishing y la manipulación de la inteligencia artificial para engañar a los usuarios y obtener acceso no autorizado a sistemas y datos.

Es importante tener en cuenta que los ataques de quinta generación no son exclusivos de las grandes empresas o gobiernos, ya que los ciberdelincuentes también pueden utilizar estas técnicas para realizar ataques dirigidos contra empresas más pequeñas o individuos. Es por eso que, es importante estar alerta y tomar medidas proactivas para protegerse contra estos ataques.

El mundo tal y como lo conocemos ha cambiado. Las empresas como Calculaser buscan formas de conectarse de forma fiable, escalar rápidamente y proteger a sus empleados locales y móviles. Al mismo tiempo, los actores de las amenazas no pierden detalle.

Según el Informe de Ciberseguridad 2022, los proveedores de software experimentaron el mayor crecimiento interanual en 2021, con un aumento del 146% desde el año 2020. Esto quizás no sea sorprendente si tenemos en cuenta que el año 2020 terminó con el ataque a la cadena de suministro de SolarWinds.

En 2021, Educación y Salud fueron los sectores más atacados, además del resurgimiento de Emotet, como una de las redes de bots más peligrosas de la historia.

Si analizamos el panorama actual la gran mayoría de las pequeñas y mediana industrias se encuentran en un nivel 3 en la escala.

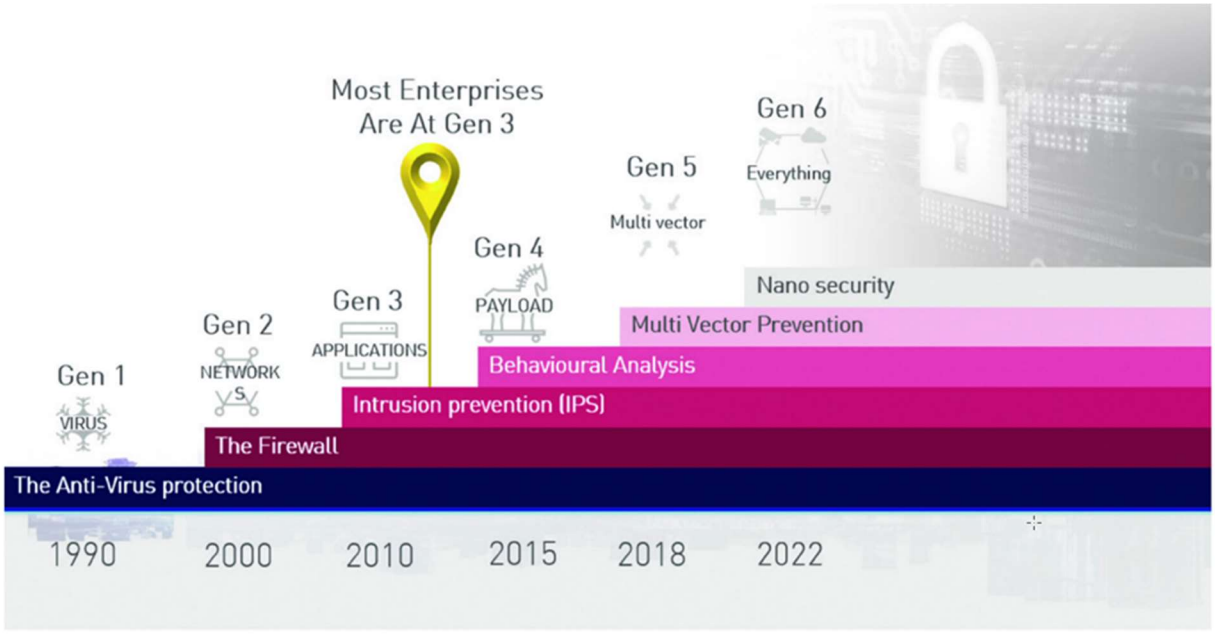


Figura 38. Evolución de la protección

Los ataques de tercera generación son aquellos que se enfocan en explotar vulnerabilidades en la estructura y protocolos de la red, en lugar de enfocarse en vulnerabilidades en los sistemas y aplicaciones individuales. Estos ataques incluyen técnicas avanzadas de piratería informática que aprovechan las debilidades de los protocolos de red y los dispositivos de red para acceder y comprometer la red.

Entre los tipos de ataques de tercera generación se incluyen:

- Ataques de denegación de servicio distribuido (DDoS): Estos ataques se basan en el uso de múltiples dispositivos para inundar un sitio web o sistema de red con tráfico malintencionado, lo que resulta en una interrupción del servicio para los usuarios legítimos.

- Ataques de inyección SQL: Estos ataques utilizan técnicas para insertar código malicioso en una base de datos a través de una consulta SQL, lo que permite a los atacantes acceder y manipular datos sensibles.

- Ataques de spoofing: Estos ataques implican falsificar información de dirección IP o MAC para hacer que parezca que el tráfico malicioso proviene de una fuente legítima.

- Ataques de sniffing: Estos ataques se centran en interceptar y leer el tráfico de red en busca de información sensible, como nombres de usuario y contraseñas.

- Ataques de secuestro de sesión: Estos ataques implican tomar el control de una sesión de usuario legítimo y utilizarla para realizar actividades maliciosas.

En general, los ataques de tercera generación son más avanzados y difíciles de detectar que los ataques de generaciones anteriores. Para mitigar estos riesgos, es importante implementar medidas de seguridad de red adecuadas, como cortafuegos, sistemas de detección de intrusiones y autenticación de usuarios.

Además, la educación de los usuarios finales y la implementación de políticas de seguridad sólidas también son críticos para prevenir estos tipos de ataques.

Conclusiones

Gracias al desarrollo de este trabajo y mediante la técnica de investigación descriptiva, se logró elaborar un inventario de activos de información clasificados como hardware, software y servicios tecnológicos que posee Calculaser SA, donde se logró identificar los activos de información de mayor criticidad.

Con el fin de valorar el grado de riesgo para los activos de información se hizo uso de la norma ISO 27005:2011 usando el análisis de riesgos para identificar las amenazas y las vulnerabilidades a las que pueden estar expuestos.

Parte del resultado muestra la identificación de 41 riesgos en zona extrema que después de realizar el proceso de tratamiento de riesgos 39 de estos se van a mitigar con controles y 3 se van a asumir.

Por tal razón es necesario la implementación de la arquitectura en ciberseguridad, que debe ir acompañada del compromiso de gerencia para que se puedan obtener los resultados esperados y así poder garantizar que la infraestructura tecnológica de Calculaser está preparada para mitigar un ataque motivo de la materialización de alguno de los riesgos.

En Colombia se hace necesario continuar trabajando en legislación para que se regulen los continuos ataques cibernéticos y las empresas dejen de temer al notificar de manera pública.

Recomendaciones

Incrementar el nivel de sensibilización de la organización en temas relacionados con ciberseguridad, riesgo tecnológico y el impacto que estos podrían generar sobre

los objetivos del negocio.

Dado la criticidad de los activos de información es necesario que Calculaser amplíe el personal de apoyo TI teniendo en cuenta que si adopta la postura de ciberseguridad diseña estas herramientas requieren demasiado esfuerzo en el monitoreo

Referencias Bibliográficas

- (1) Guerrero,W.(2014).DOCUMENTO CONPES 3701 LINEAMIENTOS DE POLÍTICAS PARA CIBERSEGURIDAD Y CIBERDEFENSA [Tesis de especialización].Universidad Piloto de Colombia. Bogota [Trabajo de tesis, última consulta Marzo 25/2023].
- (2) Colombia, R(2011, Julio 14) Documento Conpes 3701 Lineamientos de polític para ciberseguridad y ciberdefensa, https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf
- (3) Serrano,H (2009, Enero 05) Ley 1273 de 2009, https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf [Pagina web, última consulta Marzo 25/2023].
- (4) Peréz,Y(2016, Junio). Importancia de la ciberseguridad en Colombia [archivo PDF]. Recuperado de http://polux.unipiloto.edu.co:8080/00003620.pdf
- (5) Gantiva, C. (2023/02/13). La importancia de impulsar csirts sectoriales en Colombia https://urosario.edu.co/revista-nova-et-vetera/omnia/la-importancia-de-impulsar-csirts-sectoriales-en-colombia#_ftn2 [Artículo web, última consulta Marzo 30/2023]
- (6) Fuerzas militares Colombia. (s.f). CCOCI, ¿Qué hacemos?.Recuperado de https://www.ccoci.mil.co/Quienes-somos/ccoci
- (7) Gómez, Mónica. (2018, Junio 07). Así trabaja el centro cibernético Policial , https://www.canalinstitucional.tv/noticias/asi-trabaja-el-centro-cibernetico-policial
- (8) Rincón, E(2014, Junio). Instrumentos normativos de ciberseguridad [archivo PDF]. Recuperado de Normativa colombiana en materia de ciberseguridad y ciberdefensa (certicamara.com)
- (9) Lesmes,L.(Ene/24/2023).¿Qué pasa con la ciberseguridad en las plataformas de salud de Colombia?, https://www.eltiempo.com/tecnosfera/novedades-

tecnologia/ciberseguridad-en-las-plataformas-de-salud-de-colombia-736510 [Pagina web, última consulta Marzo 20/2023].

- (10) Portafolio,P(Dic/13/2022). Keralty y EPM, las más recientes víctimas de ciberataques,https://www.portafolio.co/economia/finanzas/kerealty-y-las-empresas-publicas-de-medellin-las-ultimas-victimas-de-ciberataques-575577 [Pagina web, última consulta Marzo 20/2023]
- (11) Wagner,J.(Dic/01/2022). Los hackers atacan al sistema de salud de colombia con ransomware, https://www.cibertip.com/hacking-incidentes/los-hackers-atacan-al-sistema-de-salud-de-colombia-con-ransomware/ [Página web, última consulta Marzo 20/2023]
- (12) Colombia ocupó el puesto 81 en seguridad cibernética.(2022,Abril 18). Recuperado de Colombia ocupó el puesto 81 en seguridad cibernética | Agenciapi.co
- (13)Lesmes,L. (Dic/04/2022). Keralty, la nueva víctima de los ataques de 'ransomware',https://www.eltiempo.com/tecnosfera/novedades-tecnologia/keralty-detalles-del-ataque-de-ransomware-a-eps-sanitas-723175 [Página web, última consulta Marzo 20/2023]
- (14) Puertolas. A (Abr/04/2022).Lapsus$, REvil o Anonymous: quién hay detrás de estos grupos de ciberdelincuentes que atacan a nivel mundial, https://www.20minutos.es/tecnologia/ciberseguridad/lapsus-revil-o-anonymous-quien-hay-detras-de-estos-grupos-de-ciberdelincuentes-que-atacan-a-nivel-mundial-4988115/ [Pagina web, última consulta Marzo 30/2023]
- (15) Pastor,J.(2023,Marzo 07) Qué es y cómo actúa RansomHouse, el grupo teóricamente responsable del ciberataque al Clínic de Barcelona,

https://www.xataka.com/seguridad/que-como-actua-ransomhouse-grupo-teoricamente-responsable-ciberataque-al-clinic-barcelona

- (16) Las 34 empresas que fueron hackeadas en colombia durante 2022.(2023,Enero 2). Recuperado de Las 34 empresas que fueron hackeadas en Colombia durante 2022 - Infobae
- (17) Infortec,I (2022,Diciembre) Life cycle of a ransomware incident [Archivo PDF].Recuperado de https://www.infortec.co/nosotros/
- (18) Flores,C(Dic/13/2022). TIPOS DE HACKERS.Universidad mayor de San Andres https://ns2.elhacker.net/descargas/manuales/Hacking%20y%20Seguridad%20informatica/06.%20Tipos%20de%20hackers%20(Articulo)%20autor%20Carlos%20Alberto%20Flores%20Quispe.pdf [Pagina web, última consulta Marzo 30/2023]
- (19) Dirección de Investigación criminal e Interpol Centro Cibernético Policial, Cyber noticias(2023, Enero). Recuperado de https://caivirtual.policia.gov.co/sites/default/files/observatorio/Bolet%C3%ADn%20Centro%20Cibern%C3%A9tico%20Semana%201%20de%202023_0.pdf
- (20) Dirección de Investigación criminal e Interpol Centro Cibernético Policial, Cyber noticias(2023, Febrero). Recuperado de https://caivirtual.policia.gov.co/sites/default/files/observatorio/Bolet%C3%ADn%20Centro%20Cibern%C3%A9tico%20Semana%206%20de%202023_0.pdf
- (21) Dirección de Investigación criminal e Interpol Centro Cibernético Policial, Cyber noticias(2023, Enero). Recuperado de https://caivirtual.policia.gov.co/sites/default/files/observatorio/Bolet%C3%ADn%20Centro%20Cibern%C3%A9tico%20Semana%202%20de%202023_0.pdf

Anexo A. Procedimiento de Gestión de Activos

PROCEDIMIENTO DE GESTIÓN DE CAMBIOS EN TI

1. OBJETIVO

Definir un procedimiento para gestionar las solicitudes de cambios relacionadas a cualquier modificación o mejora en la infraestructura que intervienen en la operación de Calculaser SA con el fin de tener control y claridad de los pasos a seguir y minimizar el impacto por los incidentes presentados

2. ALCANCE

El presente procedimiento se debe seguir para las solicitudes de cambio de todo el hardware, software y servicios tecnológicos que se usan en la empresa. El procedimiento inicia con la solicitud del cambio y finaliza con la entrega del cambio realizado por los responsables asignados.

3. DEFINICIONES

Cambio: Referente a cualquier adición, eliminación, modificación temporal o permanente realizada a un sistema existente.

- **Cambios Significativos:** es aquel tipo de cambio con un impacto alto, que modifica de forma sustancial el estado inicial y, por ello, requiere de una serie de actividades al finalizar su ejecución para validar que el nivel de seguridad sigue siendo consistente. Algunos ejemplos de cambios significativos

    - Instalación de un service pack o de un cambio de versión radical a nivel de sistema operativo, protocolo o aplicación.
    - Instalación de un nuevo servidor, equipo de red o base de datos en el entorno.

- Cambios en los controles de segmentación del entorno.
- Migración de tecnologías.
- Cambio de ubicación física («datacenter»).
-

4. RESPONSABLES

Apoyo TI bajo la responsabilidad de Gestión Gerencial

5. DESARROLLO

No	Actividad	Flujograma	Responsable	Registro
1	Realizar la solicitud del cambio	Solicitud del cambio	Usuario quien solicita el cambio	Diligenciar el formato de solicitud de Cambio.
2	Evaluar la solicitud del cambio y determinar si es clara la solicitud, en caso de requerir aclaración se debe informar a la persona que solicitó el cambio.	Evaluar el documento de la solicitud del cambio	Persona responsable de recibir las solicitudes del control de cambios.	Visto bueno al documento del cambio

3	Realizar una evaluación técnica del cambio para determinar si es viable su ejecución. (Evaluar impacto y riesgos de su ejecución) Como resultado de esta evaluación se determina si se aprueba o no el cambio. Cuando son cambios significativos y afectan la operación transaccional se deben validar en detalle los componentes de seguridad afectados.	Evaluación Técnica.	Apoyo TI bajo responsabilidad de Gestión gerencial	Aprobación o no del cambio. Formato de solicitud de cambio diligenciado correctamente marcando si es significativo o no.
4	Asignar las actividades a desarrollar a un responsable para su ejecución.	Asignar Actividades	Apoyo TI	Control de cambio asignado a un responsable.
5	Definir las actividades a desarrollar para ejecutar el cambio solicitado.	Definir Actividades	Persona encargada de ejecutar el cambio.	Diligenciar el formato de solicitud de Cambio

6	Notificar a todos los interesados sobre la ejecución del cambio.	Se notifica a la persona que solicitó el cambio y a todos los interesados sobre la ejecución del mismo.	Persona TI	Envío de correo para notificar la ejecución del cambio.

6. DOCUMENTOS RELACIONADOS

FT_Gestion_Cambio_TI.xlsx

7. CONTROL DE CAMBIOS DEL DOCUMENTO

Número Versión	Fecha	Resumen Cambios	Responsable	Aprobado Por
1.0		Creación Documento	Apoyo TI	Gestión Gerencial

Anexo B. Formato de Gestión de Cambios

Calculaser S.A.	GESTION DE CAMBIOS EN TI	V. 1.0

1. DATOS DE QUIEN SOLICITA			
Fecha:	DD/MM/AAAA	Dependencia:	
Solicitante		Cargo:	

2. SELECCIONE CON UNA (X) EL TIPO DE CAMBIO			
Actualizacion S.O		Mantenimiento Software	
Soporte		Parche de Seguridad	
Infraestructura Red		Otro	

3. CATEGORIA (IMPACTO DEL CAMBIO)			
Para marcar un cambio como Significativo se debe tener en cuenta que tenga un impacto alto que pueda llegar a afectar la seguridad en todo el alcance de los sistemas, por ello, requiere de una serie de actividades al finalizar su ejecución para validar que el nivel de seguridad sigue siendo consistente.			
Menor		Mayor (Significativo)	

4. PRIORIDAD (EN FUNCION DEL TIEMPO)			
Estandar		Normal	
Urgente			

5. DESCRIPCION DE LA SOLICITUD
<Breve descripcion del cambio a realizar>

6. JUSTIFICACION DEL CAMBIO
<En este espacio se debe registrar la Justificacion del cambio>

7. ACTIVO AL CUAL SE APLICA EL CAMBIO			
Marca el/los activos a los que se aplicará al gestión de cambios.			
Servidor Zeus		ERP / Yeminus	
HIS / Isalud		Firewall (Admin)	
Firewall (Asis)		Plataforma TolP	
Plataforma C.Center			

8.CONFIGURACION MODIFICADA	
En este espacio se debe detallar los cambios o configuraciones realizadas para dar atencón al cambio solicitado	
Responsable de la Modificacion	<Nombre de la persona que realizo la modificación>

9. OBSERVACIONES O RECOMENDACIONES
En este espacio se debe ingresar cualquier observacion o recomendacion a tener en cuenta en la ejecución del cambio

10. INFORMACION DE APROBACION	
Nota: La siguiente informacion solo debe ser diligenciada por la persona responsable de aprobar el cambio	
Aprobado por	< se debe ingresar el nombre completo de la persona que aprueba>
Responsable Ejecuc.	<Se debe ingresar el nombre completo de la persona responsable de ejecutar el cambio>
Cargo	
Correo	
Tiempo Estimado	<Ingresar el tiempo en horas que se requieren para la ejecución del cambio>
Fecha y Hora de Ejecución	< Fecha en que se estima ejecutar el cambio >

Firma de quien Aprueba	Firma del Responsable de la ejecución.

Anexo C. Evaluación de Amenazas

AMENAZAS		ACTIVOS (Para cada activo seleccione las amenazas que le pueden aplicar)					
	Descripción	HIS / ISalud	Plataforma de Call Center	Correo - Google Workspace	Firewall(Asis)	Srv-Zeus	Firewall(Adm)
A1	Fuego	-	-	-	X	X	X
A5	La destrucción de los equipos o medios	-	-	-	X	X	X
A6	El polvo, la corrosión, la congelación	-	-	-	X	X	X
A7	Fenómeno climático	-	-	-	-	X	-
A11	Inundación	-	-	-	X	X	X
A12	La falta de aire acondicionado o el sistema de suministro de agua	-	-	-	X	X	X
A13	La pérdida de la fuente de alimentación	-	-	-	X	X	X
A14	La falta de equipo de telecomunicaciones (Canales Datos, MPLS, Internet)	X	X	X	X	X	X
A20	Escuchas ilegales	-	X	-	-	-	-
A22	Robo de equipos	-	-	-	X	X	X
A26	La manipulación de hardware	-	-	-	X	X	X
A27	La manipulación de software	X	X	-	X	X	X
A29	Falla en el equipo	-	-	-	X	X	X
A30	Mal funcionamiento del equipo	-	-	-	X	X	X
A31	La saturación del sistema de información	X	X	-	-	-	-
A32	Mal funcionamiento de software	X	X	-	X	X	X
A33	El incumplimiento de la mantenibilidad del sistema de información	X	X	-	-	-	-
A34	El uso no autorizado de equipos	-	-	-	-	-	-
A36	El uso de software falsificado o copiado	-	-	-	-	-	-
A37	La corrupción de los datos	X	-	X	X	X	X
A39	Error en uso	X	X	X	X	X	X
A44	Ataques de identificación y autenticación de usuarios.	X	X	-	X	X	X
A46	Inadecuada configuración de la aplicación y/o sistemas.	X	X	-	X	X	X
A47	Interrupción continua de sesiones de trabajo.	X	X	X	-	-	-
A48	Desbordamiento de buffer de memoria.	-	-	-	X	X	X
A49	Inyección SQL a las aplicaciones web.	X	-	-	-	-	-
A50	Configuración incorrecta en los mensajes de error.	X	X	-	-	-	-
A51	Revelación de datos sensibles originados por eventos de SQL Inyección.	X	-	-	-	-	-
A53	Ataques de denegación de servicios.	X	X	X	X	X	X
A54	Ataques a los sistemas de detección de intrusos (IDS) y Firewalls.	-	-	-	X	-	X
A56	Escucha de puertos abiertos (Fingerprinting).	-	-	-	X	X	X
A57	Secuestro de sesión realizados por Hijacking y Man in the middle.	X	X	X	-	-	-
A58	Phising (Suplantación de identidad).	X	X	X	-	-	-
A60	Acceso no autorizado a los equipos de cómputo y/o servidores.	-	-	-	-	X	-
A61	Ataques a contraseñas de los equipos de cómputo y/o servidores.	-	-	-	-	X	
A62	Ataques de denegación de servicios Distribuidos.	X	X	X	X	-	X
A63	Ataques de ejecución de código.	X	-	-	-	-	-
A64	Ataques de Footprinting.	-	-	-	-	-	-
A65	Ataques de Malware.	X	X	X	X	X	X
A66	Ataques de puerta trasera (Backdoors).	-	-	-	-	X	-
A67	Ataques de seguridad física.	-	-	-	X	X	X
A68	Escalamiento de privilegios.	X	X	X	X	X	X
A70	Indisponibilidad en el servicio de VPN	-	-	-	X	-	X

Anexo D. Vulnerabilidades y Método

ANEXO D - Vulnerabilidades y métodos para la evaluación de la vulnerabilidad			
Tipo de Activo	Código	Descripción de la vulnerabilidad	Amenazas
Hardware	V1	Mantenimiento insuficiente / instalación defectuosa de medios de almacenamiento	Incumplimiento en el mantenimiento del sistema de información
	V2	La falta de planes de sustitución periódicas	La destrucción de los equipos o medios
	V3	La susceptibilidad a la humedad, el polvo, la suciedad	El polvo, la corrosión, la congelación
	V4	Sensibilidad a la radiación electromagnética	Radiación electromagnética
	V5	La falta de control de cambio de configuración eficiente	Error en uso
	V6	La susceptibilidad a las variaciones de voltaje	La pérdida de la fuente de alimentación
	V7	La susceptibilidad a las variaciones de temperatura	Fenómeno meteorológico
	V8	Almacenamiento sin protección	El robo de los medios de comunicación o documentos
	V9	La falta de atención a la disposición	El robo de los medios de comunicación o documentos
	V10	La copia no controlada	El robo de los medios de comunicación o documentos
Software	V11	No hay pruebas de software o insuficiente	Abuso de los derechos
	V12	Defectos conocidos en el software	Abuso de los derechos
	V13	No 'Cerrar sesión' al salir de la estación de trabajo	Abuso de los derechos
	V14	Eliminación o reutilización de los medios de almacenamiento sin borrado adecuada	Abuso de los derechos
	V15	La falta de seguimiento de auditoría	Abuso de los derechos
	V16	La asignación de derechos de acceso incorrecto	Abuso de los derechos
	V17	Software distribuido ampliamente	La corrupción de los datos
	V18	En terminos de tiempo utilizacion de datos errados en los programas de aplicación	La corrupción de los datos
	V19	Interfaz de usuario complicada	Error en uso
	V20	La falta de documentación	Error en uso
	V21	Parámetro incorrecto configurado	Error en uso
	V22	Fechas incorrectas	Error en uso
	V23	La falta de mecanismos de identificación y autenticación como la autenticación de usuarios	Falsificacion de derechos
	V24	Tablas de contraseñas no protegidas	Falsificacion de derechos
	V25	La mala gestión de contraseñas	Falsificacion de derechos
	V26	Servicios innecesarios habilitadas	Procesamiento ilegal de datos
	V27	Software inmadura o una nueva	Mal funcionamiento de software
	V28	Especificaciones confusas o incompletas para desarrolladores	Mal funcionamiento de software
	V29	La falta de control de cambio de efectivo	Mal funcionamiento de software
	V30	La descarga incontrolada y uso del software	La manipulación de software
	V31	La falta de copias de seguridad	La manipulación de software
	V32	La falta de protección física de los edificios, puertas y ventanas	El robo de los medios de comunicación o documentos
	V33	Falta de presentación de informes de gestión	El uso no autorizado de equipos
Red	V34	La falta de prueba de envío o recepción de un mensaje	La negación de las acciones
	V35	Líneas de comunicación no protegidos	Escuchas ilegales
	V36	El tráfico sensible sin protección	Escuchas ilegales
	V37	Cableado deficiente conjunta	La falta de equipo de telecomunicaciones
	V38	Punto único de fallo	La falta de equipo de telecomunicaciones
	V39	La falta de identificación y autenticación de remitente y el receptor	Falsificacion de derechos
	V40	Arquitectura de red insegura	Espionaje remoto
	V41	Transferencia de contraseñas en claro	Espionaje remoto
	V42	Inadequatenetworkmanagement (resiliencia de enrutamiento)	La saturación del sistema de información
	V43	Conexiones de red pública no protegidos	El uso no autorizado de equipos

Tipo de Activo	Código	Descripción de la vulnerabilidad	Amenazas
Personal	V44	Ausencia de personal	El incumplimiento de la disponibilidad de personal
	V45	La insuficiencia de los procedimientos de contratación	La destrucción de los equipos o medios
	V46	Formación de seguridad insuficientes	Error en uso
	V47	El uso incorrecto de software y hardware	Error en uso
	V48	La falta de conciencia de seguridad	Error en uso
	V49	La falta de mecanismos de seguimiento	Procesamiento ilegal de datos
	V50	El trabajo no supervisado por el exterior o el personal de limpieza	El robo de los medios de comunicación o documentos
	V51	La falta de políticas para el correcto uso de los medios de telecomunicaciones y mensajería	El uso no autorizado de equipos
Lugar	V52	El uso inadecuado o negligente de control de acceso físico a los edificios y recintos	La destrucción de los equipos o medios
	V53	Ubicación en un área susceptible a las inundaciones	Inundación
	V54	Red de energía inestable	La pérdida de la fuente de alimentación
	V55	La falta de protección física de los edificios, puertas y ventanas	Robo de equipos
Organización	V56	Fallas o ausencia de un procedimiento establecido para la administración, registro, modificación y retiro de usuarios.	Abuso de los derechos
	V57	Fallas o ausencia de un procedimiento o proceso establecido para la revisión y/o supervisión de los derechos de acceso de los usuarios.	Abuso de los derechos
	V58	Ausencia de cláusulas de seguridad de la información y ciberseguridad en los contratos con los colaboradores, proveedores, clientes y/o terceras partes.	Abuso de los derechos
	V59	Fallas o ausencia de procedimientos de monitoreo y/o seguimiento de los recursos de información.	Abuso de los derechos
	V60	Fallas o ausencia de auditorías periódicas.	Abuso de los derechos
	V61	Fallas o ausencia en los procedimientos de identificación y valoración de riesgos.	Abuso de los derechos
	V62	Fallas o ausencia de reportes que identifican las actividades realizadas por los administradores y usuarios de los sistemas.	Abuso de los derechos
	V63	Nivel de servicio bajo en relación al mantenimiento de los sistemas de información.	Incumplimiento en el mantenimiento del sistema de información
	V64	Fallas o ausencia de acuerdos de nivel de servicio.	Incumplimiento en el mantenimiento del sistema de información
	V66	Fallas o ausencia de un procedimiento establecido para el control de la documentación del SGSI y ciberseguridad.	Incumplimiento en el mantenimiento del sistema de información
	V67	Fallas o ausencia de un procedimiento establecido para la supervisión del registro del SGSI y ciberseguridad.	La corrupción de los datos
	V68	Fallas o ausencia de un procedimiento establecido para la autorización de la información que estará disponible de manera pública.	Datos provenientes de fuentes no cinfiables
	V69	Fallas o ausencia de la asignación adecuada de roles y responsabilidades en relación a la seguridad de la información y ciberseguridad.	La negación de las acciones
	V70	Fallas o ausencia en los planes de continuidad de negocio.	Falla en el equipo
	V71	Fallas o ausencia de políticas sobre el uso de correo electrónico, clasificación y etiquetado de la información.	Error en uso
	V72	Fallas o ausencia de procedimientos para la instalación del software en los sistemas operativos.	Error en uso
	V73	Fallas o ausencia de registro en las bitácoras (logs de administrador y operario).	Error en uso
	V74	Fallas o ausencia de procedimientos para el manejo de información sensible y/o confidencial.	Error en uso
	V75	Fallas o ausencia de responsabilidades de los cargos en relación a la seguridad de la información.	Error en uso
	V76	Fallas o ausencia en las disposiciones y/o cláusulas de los contratos de los colaboradores en relación a temas de seguridad de la información y ciberseguridad.	Procesamiento ilegal de datos
	V77	Fallas o ausencia de procesos disciplinarios definidos en el caso de incidentes de seguridad de la información y/o ciberseguridad.	Robo de equipos
	V78	Fallas o ausencia de políticas definidas sobre la utilización de computadores portátiles y/o dispositivos móviles.	Robo de equipos
	V79	Fallas o ausencia de control en relación a los activos que se encuentran fuera de las instalaciones de la organización.	Robo de equipos
	V80	Fallas o ausencia de políticas y/o procedimientos sobre la limpieza del escritorio o pantalla del equipo de cómputo.	El robo de los medios de comunicación o documentos
	V81	Fallas o ausencia de autorización en el procesamiento de la información.	El robo de los medios de comunicación o documentos
	V82	Fallas o ausencia de mecanismos de monitoreo o seguimiento para brechas en seguridad de la información y/o ciberseguridad.	El robo de los medios de comunicación o documentos
	V83	Fallas o ausencia de verificaciones periódicas por parte de los dueños de los procesos.	El uso no autorizado de equipos
	V84	Fallas o ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad de la información y/o ciberseguridad.	El uso no autorizado de equipos
	V85	Fallas o ausencia de procedimientos del cumplimiento de las disposiciones legales relacionadas con los derechos intelectuales y/o protección de datos personales.	El uso de software falsificado o copiado

Anexo E. Análisis de Riesgos

	ANÁLISIS DE RIESGOS					
	ESCENARIO DE RIESGO	PROBABILIDAD		IMPACTO		RIESGO
R1	HIS / Isalud - La falta de equipo de telecomunicaciones (Canales Datos, MPLS, Internet)	Posible	2	Moderado	3	6
R2	HIS / Isalud - La Manipulacion Software	Improbable	1	Catastrófico	5	5
R3	HIS / Isalud - La saturación del sistema de información	Probable	4	Catastrófico	5	20
R4	HIS / Isalud - Mal funcionamiento de software	Improbable	1	Menor	2	2
R5	HIS / Isalud - El incumplimiento de la mantenibilidad del sistema de información	Posible	2	Peligroso	4	8
R6	HIS / Isalud - La Corrupcion de los datos	Improbable	1	Peligroso	4	4
R7	HIS / Isalud - Error en Uso	Posible	2	Moderado	3	6
R8	HIS / Isalud - Ataques de identificación y autenticación de usuarios.	Posible	2	Moderado	3	6
R9	HIS / Isalud - Inadecuada configuración de la aplicación y/o sistemas.	Improbable	1	Moderado	3	3
R10	HIS / Isalud - Interrupción continua de sesiones de trabajo	Improbable	1	Menor	2	2
R11	HIS / Isalud - Inyección SQL a las aplicaciones web.	Frecuente	5	Catastrófico	5	25
R12	HIS / Isalud - Configuración incorrecta en los mensajes de error.	Probable	4	Insignificante	1	4
R13	HIS / Isalud - Revelación de datos sensibles originados por eventos de SQL Inyección.	Frecuente	5	Catastrófico	5	25
R14	HIS / Isalud - Ataques de denegación de servicios	Posible	2	Catastrófico	5	10
R15	HIS / Isalud - Secuestro de sesión realizados por Hijacking y Man in the middle.	Posible	2	Moderado	3	6
R16	HIS / Isalud - Phising (Suplantación de identidad).	Posible	2	Peligroso	4	8
R17	HIS / Isalud - Ataques de denegación de servicios Distribuidos.	Posible	2	Catastrófico	5	10
R18	HIS / Isalud - Ataques de ejecución de código.	Frecuente	5	Catastrófico	5	25
R19	HIS / Isalud - Ataques de malware	Improbable	1	Insignificante	1	1
R20	HIS / Isalud - Escalamiento de privilegios.	Ocasional	3	Moderado	3	9
R21	PItf CC - La falta de equipo de telecomunicaciones (Canales Datos, MPLS, Internet)	Posible	2	Moderado	3	6
R22	PItf CC - Escuchas ilegales	Posible	2	Peligroso	4	8
R23	PItf CC - La Manipulacion Software	Posible	2	Moderado	3	6
R24	PItf CC - La saturación del sistema de información	Probable	4	Catastrófico	5	20
R25	PItf CC - Mal funcionamiento de software	Improbable	1	Menor	2	2
R26	PItf CC - El incumplimiento de la mantenibilidad del sistema de información	Posible	2	Peligroso	4	8
R27	PItf CC - Error en Uso	Posible	2	Moderado	3	6
R28	PItf CC - Ataques de identificación y autenticación de usuarios.	Posible	2	Moderado	3	6
R29	PItf CC - Inadecuada configuración de la aplicación y/o sistemas.	Improbable	1	Moderado	3	3
R30	PItf CC - Interrupción continua de sesiones de trabajo	Improbable	1	Menor	2	2

	ESCENARIO DE RIESGO	PROBABILIDAD		IMPACTO		RIESGO
R31	PItf CC - Configuración incorrecta en los mensajes de error.	Ocasional	3	Insignificante	1	3
R32	PItf CC - Ataques de denegación de servicios	Posible	2	Catastrófico	5	10
R33	PItf CC - Secuestro de sesión realizados por Hijacking y Man in the middle.	Posible	2	Moderado	3	6
R34	PItf CC - Phising (Suplantación de identidad).	Posible	2	Peligroso	4	8
R35	PItf CC - Ataques de denegación de servicios Distribuidos.	Posible	2	Catastrófico	5	10
R36	PItf CC - Ataques de Malware.	Improbable	1	Insignificante	1	1
R37	PItf CC - Escalamiento de privilegios.	Ocasional	3	Moderado	3	9
R38	Google Correo - La falta de equipo de telecomunicaciones (Canales Datos, MPLS, Internet)	Posible	2	Moderado	3	6
R39	Google Correo - La Corrupcion de los datos	Frecuente	5	Peligroso	4	20
R40	Google Correo - Error en Uso	Posible	2	Moderado	3	6
R41	Google Correo - Interrupción continua de sesiones de trabajo	Improbable	1	Menor	2	2
R42	Google Correo - Ataques de denegación de servicios	Posible	2	Catastrófico	5	10
R43	Google Correo - Secuestro de sesión realizados por Hijacking y Man in the middle.	Improbable	1	Menor	2	2
R44	Google Correo - Phising (Suplantación de identidad).	Catastrófico	5	Catastrófico	5	25
R45	Google Correo - Ataques de denegación de servicios Distribuidos.	Posible	2	Catastrófico	5	10
R46	Google Correo - Ataques de Malware.	Frecuente	5	Peligroso	4	20
R47	Google Correo - Escalamiento de privilegios.	Improbable	1	Insignificante	1	1
R48	Firewall(Asis) - Fuego	Ocasional	3	Peligroso	4	12
R49	Firewall(Asis) - La destrucción de los equipos o medios	Posible	2	Peligroso	4	8
R50	Firewall(Asis) - El polvo, la corrosión, la congelación	Posible	2	Moderado	3	6
R51	Firewall(Asis) - Inundación	Ocasional	3	Catastrófico	5	15
R52	Firewall(Asis) - La falta de aire acondicionado o el sistema de suministro de agua	Improbable	1	Insignificante	1	1
R53	Firewall(Asis) - La pérdida de la fuente de alimentación	Posible	2	Menor	2	4
R54	Firewall(Asis) - La falta de equipo de telecomunicaciones (Canales Datos, MPLS, Internet)	Posible	2	Moderado	3	6
R55	Firewall(Asis) - Robo de equipos	Improbable	1	Insignificante	1	1
R56	Firewall(Asis) - La manipulacion del hardware	Improbable	1	Catastrófico	5	5
R57	Firewall(Asis) - La manipulacion del software	Improbable	1	Moderado	3	3
R58	Firewall(Asis) - Fallas en el equipo	Frecuente	5	Catastrófico	5	25
R59	Firewall(Asis) - Mal funcionamiento del equipo	Improbable	1	Catastrófico	5	5
R60	Firewall(Asis) - Mal funcionamiento del software	Improbable	1	Catastrófico	5	5

	ESCENARIO DE RIESGO	PROBABILIDAD		IMPACTO		RIESGO
R61	Firewall(Asis) - La corrupcion de los datos	Improbable	1	Insignificante	1	1
R62	Firewall(Asis) - Error en uso	Improbable	1	Insignificante	1	1
R63	Firewall(Asis) -Ataques de identificación y autenticación de usuarios.	Improbable	1	Insignificante	1	1
R64	Firewall(Asis) - Inadecuada configuración de la aplicación y/o sistemas.	Improbable	1	Insignificante	1	1
R65	Firewall(Asis) - Desbordamiento de la memoria	Ocasional	3	Catastrófico	5	15
R66	Firewall(Asis) - Ataques de denegacion de servicio	Frecuente	5	Catastrófico	5	25
R67	Firewall(Asis) - Ataques a los sistemas de detección de intrusos (IDS) y Firewalls.	Frecuente	5	Catastrófico	5	25
R68	Firewall(Asis) - Escucha de puertos abiertos (Fingerprinting).	Frecuente	5	Catastrófico	5	25
R69	Firewall(Asis) - Ataques de denegación de servicios Distribuidos.	Frecuente	5	Catastrófico	5	25
R70	Firewall(Asis) - Ataques de Malware.	Improbable	1	Insignificante	1	1
R71	Firewall(Asis) - Ataques de seguridad fisica	Improbable	1	Insignificante	1	1
R72	Firewall(Asis) - Escalamiento de privilegios.	Posible	2	Catastrófico	5	10
R73	Firewall(Asis) -Indisponibilidad en el servicio de vpn	Probable	4	Catastrófico	5	20
R74	Srv-Zeus - Fuego	Ocasional	3	Peligroso	4	12
R75	Srv-Zeus - La destrucción de los equipos o medios	Posible	2	Peligroso	4	8
R76	Srv-Zeus - El polvo, la corrosión, la congelación	Posible	2	Moderado	3	6
R77	Srv-Zeus -Fenómeno climático	Posible	2	Moderado	3	6
R78	Srv-Zeus - Inundación	Ocasional	3	Catastrófico	5	15
R79	Srv-Zeus - La falta de aire acondicionado o el sistema de suministro de agua	Ocasional	3	Menor	2	6
R80	Srv-Zeus - La pérdida de la fuente de alimentación	Posible	2	Menor	2	4
R81	Srv-Zeus - La falta de equipo de telecomunicaciones (Canales Datos, MPLS, Internet)	Posible	2	Moderado	3	6
R82	Srv-Zeus - Robo de equipos	Improbable	1	Insignificante	1	1
R83	Srv-Zeus - La manipulacion del hardware	Improbable	1	Catastrófico	5	5
R84	Srv-Zeus - La manipulacion del software	Improbable	1	Moderado	3	3
R85	Srv-Zeus - Fallas en el equiopo	Frecuente	5	Catastrófico	5	25
R86	Srv-Zeus - Mal funcionamiento del equipo	Improbable	1	Catastrófico	5	5
R87	Srv-Zeus - Mal funcionamiento del software	Improbable	1	Catastrófico	5	5
R88	Srv-Zeus - La corrupcion de los datos	Improbable	1	Insignificante	1	1
R89	Srv-Zeus - Error en uso	Improbable	1	Insignificante	1	1
R90	Srv-Zeus -Ataques de identificación y autenticación de usuarios.	Improbable	1	Insignificante	1	1

	ESCENARIO DE RIESGO	PROBABILIDAD		IMPACTO		RIESGO
R91	Srv-Zeus - Inadecuada configuración de la aplicación y/o sistemas.	Improbable	1	Insignificante	1	1
R92	Srv-Zeus - Desbordamiento de la memoria	Ocasional	3	Catastrófico	5	15
R93	Srv-Zeus - Ataques de denegacion de servicio	Frecuente	5	Catastrófico	5	25
R94	Srv-Zeus - Escucha de puertos abiertos (Fingerprinting).	Improbable	1	Insignificante	1	1
R95	Srv-Zeus - Acceso no autorizado a los equipos de cómputo y/o servidores.	Improbable	1	Menor	2	2
R96	Srv-Zeus - Ataques a contraseñas de los equipos de cómputo y/o servidores.	Improbable	1	Menor	2	2
R97	Srv-Zeus - Ataques de denegación de servicios Distribuidos.	Frecuente	5	Catastrófico	5	25
R98	Srv-Zeus - Ataques de Malware.	Improbable	1	Insignificante	1	1
R99	Srv-Zeus - Ataques de seguridad fisica	Improbable	1	Insignificante	1	1
R100	Srv-Zeus - Escalamiento de privilegios.	Posible	2	Catastrófico	5	10
R113	Firewall(Adm) - Fuego	Ocasional	3	Peligroso	4	12
R114	Firewall(Adm) - La destrucción de los equipos o medios	Posible	2	Peligroso	4	8
R115	Firewall(Adm) - El polvo, la corrosión, la congelación	Posible	2	Moderado	3	6
R116	Firewall(Adm) - Inundación	Ocasional	3	Catastrófico	5	15
R117	Firewall(Adm) - La falta de aire acondicionado o el sistema de suministro de agua	Ocasional	3	Menor	2	6
R118	Firewall(Adm) - La pérdida de la fuente de alimentación	Posible	2	Menor	2	4
R119	Firewall(Adm) - La falta de equipo de telecomunicaciones (Canales Datos, MPLS, Internet)	Posible	2	Moderado	3	6
R120	Firewall(Adm) - Robo de equipos	Improbable	1	Insignificante	1	1
R121	Firewall(Adm) - La manipulacion del hardware	Improbable	1	Catastrófico	5	5
R122	Firewall(Adm) - La manipulacion del software	Improbable	1	Moderado	3	3
R123	Firewall(Adm) - Fallas en el equipo	Catastrófico	5	Catastrófico	5	25
R124	Firewall(Adm) - Mal funcionamiento del equipo	Improbable	1	Catastrófico	5	5
R125	Firewall(Adm) - Mal funcionamiento del software	Improbable	1	Catastrófico	5	5
R126	Firewall(Adm) - La corrupcion de los datos	Improbable	1	Insignificante	1	1
R127	Firewall(Adm) - Error en uso	Improbable	1	Insignificante	1	1
R128	Firewall(Adm) -Ataques de identificación y autenticación de usuarios.	Improbable	1	Insignificante	1	1
R129	Firewall(Adm) - Inadecuada configuración de la aplicación y/o sistemas.	Improbable	1	Insignificante	1	1
R130	Firewall(Adm) - Desbordamiento de la memoria	Ocasional	3	Catastrófico	5	15
R131	Firewall(Adm) - Ataques de denegacion de servicio	Frecuente	5	Catastrófico	5	25
R132	Firewall(Adm) - Ataques a los sistemas de detección de intrusos (IDS) y Firewalls.	Frecuente	5	Catastrófico	5	25
R133	Firewall(Adm) - Escucha de puertos abiertos (Fingerprinting).	Frecuente	5	Catastrófico	5	25
R134	Firewall(Adm) - Ataques de denegación de servicios Distribuidos.	Frecuente	5	Catastrófico	5	25
R135	Firewall(Adm) - Ataques de Malware.	Improbable	1	Insignificante	1	1
R136	Firewall(Adm) - Ataques de seguridad fisica	Improbable	1	Insignificante	1	1
R137	Firewall(Adm) - Escalamiento de privilegios.	Posible	2	Catastrófico	5	10
R138	Firewall(Adm) - Indisponibilidad en el servicio de vpn	Probable	4	Catastrófico	5	20

Anexo F. Tratamiento de Riesgos

No.	Activos	Areas	Riesgos	Amenazas	Vulnerabilidades (Posible explotación)	Confidencialidad	Integridad	Disponibilidad	Operativo	Financiero	Jurídico	Sanción o multa	Imagen Reputacional	Tecnologico	Medio Ambiente	Nivel de Riesgo (Probabilidad x Consecuencia)	Estrategia (Mitigar, Asumir, Transferir, Eliminar)
1	HIS / Isalud	Gestion Asistencial Gestion Prestacion Servicios	Ataques a sitios o aplicaciones web.	Inyección SQL a las aplicaciones web.	Parámetro incorrecto configurado	Baja	Baja	Alta	4 - Severo	2 - Menor	5 - Crítico	5 - Crítico	3 - Dañino	2 - Menor	1 - Insignificante	Extremo	Mitigar
			Perdida de información confidencial y/o sensible por acceso no autorizado y/o ausencia de controles.	Recolección de datos sensibles originados por eventos de SQL Injection.	El tráfico sensible sin protección	Baja	Alta	Alta	3 - Dañino	2 - Menor	5 - Crítico	5 - Crítico	3 - Dañino	2 - Menor	1 - Insignificante	Extremo	Mitigar
			Acceso a los sistemas de información o recursos tecnológicos por usuarios no autorizados.	Ataques de ejecución de código.	Parámetro incorrecto configurado	Baja	Baja	Alta	4 - Severo	4 - Severo	3 - Dañino	5 - Crítico	4 - Severo	4 - Severo	1 - Insignificante	Extremo	Mitigar
2	Google Correo	Toda la Organizacion	Acceso a los sistemas de información o recursos tecnológicos por usuarios no autorizados.	Phising (Suplantacion de identidad).	La falta de identificación y autenticación de remitente y el receptor	Baja	Alta	Alta	2 - Menor	2 - Menor	2 - Menor	2 - Menor	2 - Menor	4 - Severo	1 - Insignificante	Extremo	Mitigar
3	Firewall(Asis)	Gerencia	Daño al centro de procesamiento de datos y/o servidores.	Falla en el equipo	Red de energía inestable	Alta	Alta	Baja	5 - Crítico	3 - Dañino	1 - Insignificante	1 - Insignificante	1 - Insignificante	3 - Dañino	1 - Insignificante	Extremo	Mitigar
			Afectación de la continuidad de la operación por fallas en los sistemas de información.	Ataques de denegación de servicios.	Arquitectura de red inegura	Alta	Alta	Baja	4 - Severo	2 - Menor	1 - Insignificante	1 - Insignificante	3 - Dañino	4 - Severo	1 - Insignificante	Extremo	Mitigar
			Fallas en los procesos tecnológicos.	Ataques a los sistemas de detección de intrusos (IDS) y Firewalls.	Parámetro incorrecto configurado	Alta	Alta	Baja	4 - Severo	2 - Menor	1 - Insignificante	1 - Insignificante	3 - Dañino	4 - Severo	1 - Insignificante	Extremo	Mitigar
			Errores en la configuración y/o parametrización de la infraestructura tecnológica.	Escucha de puertos abiertos (Fingerprinting).	Servicios innecesarios habilitados	Baja	Alta	Alta	3 - Dañino	2 - Menor	5 - Crítico	2 - Menor	2 - Menor	3 - Dañino	1 - Insignificante	Extremo	Mitigar
			Afectación de la continuidad de la operación por fallas en los sistemas de información.	Ataques de denegación de servicios.	Arquitectura de red inegura	Alta	Alta	Baja	4 - Severo	2 - Menor	1 - Insignificante	1 - Insignificante	3 - Dañino	4 - Severo	1 - Insignificante	Extremo	Mitigar
4	Srv-Zeus	Gerencia	Daño al centro de procesamiento de datos y/o servidores.	Falla en el equipo	Mantenimiento inadecuado / instalación defectuosa de medios de almacenamiento	Alta	Alta	Baja	5 - Crítico	3 - Dañino	1 - Insignificante	1 - Insignificante	1 - Insignificante	3 - Dañino	1 - Insignificante	Extremo	Mitigar
			Afectación de la continuidad de la operación por fallas en los sistemas de información.	Ataques de denegación de servicios.	Arquitectura de red inegura	Alta	Alta	Baja	4 - Severo	2 - Menor	1 - Insignificante	1 - Insignificante	3 - Dañino	4 - Severo	1 - Insignificante	Extremo	Mitigar
			Afectación de la continuidad de la operación por fallas en los sistemas de información.	Ataques de denegación de servicios Distribuidos.	Arquitectura de red inegura	Alta	Alta	Baja	4 - Severo	2 - Menor	1 - Insignificante	1 - Insignificante	3 - Dañino	4 - Severo	1 - Insignificante	Extremo	Mitigar
5	Firewall(Admi)	Gerencia	Daño al centro de procesamiento de datos y/o servidores.	Falla en el equipo	Red de energía inestable	Alta	Alta	Baja	5 - Crítico	3 - Dañino	1 - Insignificante	1 - Insignificante	1 - Insignificante	3 - Dañino	1 - Insignificante	Extremo	Mitigar
			Afectación de la continuidad de la operación por fallas en los sistemas de información.	Ataques de denegación de servicios.	Arquitectura de red inegura	Alta	Alta	Baja	4 - Severo	2 - Menor	1 - Insignificante	1 - Insignificante	3 - Dañino	4 - Severo	1 - Insignificante	Extremo	Mitigar
			Fallas en los procesos tecnológicos.	Ataques a los sistemas de detección de intrusos (IDS) y Firewalls.	Parámetro incorrecto configurado	Alta	Alta	Baja	4 - Severo	2 - Menor	1 - Insignificante	1 - Insignificante	3 - Dañino	4 - Severo	1 - Insignificante	Extremo	Mitigar
			Errores en la configuración y/o parametrización de la infraestructura tecnológica.	Escucha de puertos abiertos (Fingerprinting).	Servicios innecesarios habilitados	Baja	Alta	Alta	3 - Dañino	2 - Menor	5 - Crítico	2 - Menor	2 - Menor	3 - Dañino	1 - Insignificante	Extremo	Mitigar
			Afectación de la continuidad de la operación por fallas en los sistemas de información.	Ataques de denegación de servicios.	Arquitectura de red inegura	Alta	Alta	Baja	4 - Severo	2 - Menor	1 - Insignificante	1 - Insignificante	3 - Dañino	4 - Severo	1 - Insignificante	Extremo	Mitigar
6	Google Correo	Gerencia	Soporte inadecuado.	La corrupcion de los datos	Parametro incorrecto configurado	Moderada	Baja	Baja	4 - Severo	3 - Dañino	1 - Insignificante	1 - Insignificante	1 - Insignificante	3 - Dañino	1 - Insignificante	Extremo	Mitigar
			Ataques de virus.	Ataques de Malware.	Formación de seguridad insuficientes	Baja	Baja	Baja	5 - Crítico	3 - Dañino	1 - Insignificante	1 - Insignificante	1 - Insignificante	4 - Severo	1 - Insignificante	Extremo	Mitigar
7	HIS / Isalud	Gestion Asistencial Gestion Prestacion Servicios	Afectación de la continuidad de la operación por fallas en los sistemas de información.	La saturación del sistema de información	No hay pruebas de software o insuficiente	Alta	Alta	Baja	4 - Severo	3 - Dañino	3 - Dañino	3 - Dañino	3 - Dañino	4 - Severo	1 - Insignificante	Extremo	Mitigar
8	PBFCC	Gestion Prestacion Servicios	Afectación de la continuidad de la operación por fallas en los sistemas de información.	La saturación del sistema de información	No hay pruebas de software o insuficiente	Alta	Alta	Baja	4 - Severo	3 - Dañino	3 - Dañino	3 - Dañino	3 - Dañino	4 - Severo	1 - Insignificante	Extremo	Mitigar
9	Firewall(Asis)	Gerencia	Afectación de la continuidad de la operación por fallas en los sistemas de información.	Indisponibilidad en el servicio de VPN	Fallas o ausencia en los planes de continuidad de negocio.	Alta	Alta	Baja	4 - Severo	1 - Insignificante	1 - Insignificante	1 - Insignificante	1 - Insignificante	4 - Severo	1 - Insignificante	Extremo	Mitigar
10	Firewall(Admi)	Gerencia	Afectación de la continuidad de la operación por fallas en los sistemas de información.	Indisponibilidad en el servicio de VPN	Fallas o ausencia en los planes de continuidad de negocio.	Alta	Alta	Baja	4 - Severo	1 - Insignificante	1 - Insignificante	1 - Insignificante	1 - Insignificante	4 - Severo	1 - Insignificante	Extremo	Mitigar
11	Firewall(Asis)	Gerencia	Daño al centro de procesamiento de datos y/o servidores.	Inundación	Ubicación en un área susceptible a las inundaciones.	Alta	Alta	Baja	3 - Dañino	5 - Crítico	1 - Insignificante	1 - Insignificante	1 - Insignificante	4 - Severo	1 - Insignificante	Extremo	Asumir
			Afectación de la continuidad de la operación por fallas en los sistemas de información.	Desbordamiento de buffer de memoria.	Fallas o ausencia en los planes de continuidad de negocio.	Alta	Alta	Baja	4 - Severo	3 - Dañino	1 - Insignificante	1 - Insignificante	1 - Insignificante	4 - Severo	1 - Insignificante	Extremo	Mitigar
12	Srv-Zeus	Gerencia	Daño al centro de procesamiento de datos y/o servidores.	Inundación	Ubicación en un área susceptible a las inundaciones.	Alta	Alta	Baja	3 - Dañino	5 - Crítico	1 - Insignificante	1 - Insignificante	1 - Insignificante	4 - Severo	1 - Insignificante	Extremo	Asumir
			Error en la calidad e integridad de la información.	Inadecuada configuración de la aplicación y/o sistemas.	La falta de control de cambio de configuración efectiva	Alta	Baja	Alta	3 - Dañino	4 - Severo	3 - Dañino	1 - Insignificante	1 - Insignificante	3 - Dañino	1 - Insignificante	Extremo	Mitigar
13	Firewall(Admi)	Gerencia	Daño al centro de procesamiento de datos y/o servidores.	Inundación	Ubicación en un área susceptible a las inundaciones.	Alta	Alta	Baja	3 - Dañino	5 - Crítico	1 - Insignificante	1 - Insignificante	1 - Insignificante	4 - Severo	1 - Insignificante	Extremo	Asumir
			Afectación de la continuidad de la operación por fallas en los sistemas de información.	Desbordamiento de buffer de memoria.	Fallas o ausencia en los planes de continuidad de negocio.	Alta	Alta	Baja	4 - Severo	3 - Dañino	1 - Insignificante	1 - Insignificante	1 - Insignificante	4 - Severo	1 - Insignificante	Extremo	Mitigar
14	Firewall(Asis)	Gerencia	Daño al centro de procesamiento de datos y/o servidores.	Fuego	La falta de protección física de los edificios, puertas y ventanas	Alta	Alta	Baja	3 - Dañino	5 - Crítico	1 - Insignificante	3 - Dañino	2 - Menor	4 - Severo	4 - Severo	Extremo	Mitigar
15	Srv-Zeus	Gerencia	Daño al centro de procesamiento de datos y/o servidores.	Fuego	La falta de protección física de los edificios, puertas y ventanas	Alta	Alta	Baja	3 - Dañino	5 - Crítico	1 - Insignificante	3 - Dañino	2 - Menor	4 - Severo	4 - Severo	Extremo	Mitigar
16	Firewall(Admi)	Gerencia	Daño al centro de procesamiento de datos y/o servidores.	Fuego	La falta de protección física de los edificios, puertas y ventanas	Alta	Alta	Baja	3 - Dañino	5 - Crítico	1 - Insignificante	3 - Dañino	2 - Menor	4 - Severo	4 - Severo	Extremo	Mitigar
17	HIS / Isalud	Gestion Asistencial Gestion Prestacion Servicios	Afectación de la continuidad de la operación por fallas en los sistemas de información.	Ataques de denegación de servicios.	Arquitectura de red inegura	Alta	Alta	Baja	4 - Severo	2 - Menor	1 - Insignificante	1 - Insignificante	3 - Dañino	4 - Severo	1 - Insignificante	Extremo	Mitigar
			Afectación de la continuidad de la operación por fallas en los sistemas de información.	Ataques de denegación de servicios Distribuidos.	Arquitectura de red inegura	Alta	Alta	Baja	4 - Severo	2 - Menor	1 - Insignificante	1 - Insignificante	3 - Dañino	4 - Severo	1 - Insignificante	Extremo	Mitigar
18	PBFCC	Gestion Prestacion Servicios	Afectación de la continuidad de la operación por fallas en los sistemas de información.	Ataques de denegación de servicios.	Arquitectura de red inegura	Alta	Alta	Baja	4 - Severo	2 - Menor	1 - Insignificante	1 - Insignificante	3 - Dañino	4 - Severo	1 - Insignificante	Extremo	Mitigar
19	Google Correo	Gerencia	Afectación de la continuidad de la operación por fallas en los sistemas de información.	Ataques de denegación de servicios Distribuidos.	Arquitectura de red inegura	Alta	Alta	Baja	4 - Severo	2 - Menor	1 - Insignificante	1 - Insignificante	3 - Dañino	4 - Severo	1 - Insignificante	Extremo	Mitigar
			Afectación de la continuidad de la operación por fallas en los sistemas de información.	Ataques de denegación de servicios.	Arquitectura de red inegura	Alta	Alta	Baja	4 - Severo	2 - Menor	1 - Insignificante	1 - Insignificante	3 - Dañino	4 - Severo	1 - Insignificante	Extremo	Mitigar
			Afectación de la continuidad de la operación por fallas en los sistemas de información.	Ataques de denegación de servicios Distribuidos.	Arquitectura de red inegura	Alta	Alta	Baja	4 - Severo	2 - Menor	1 - Insignificante	1 - Insignificante	3 - Dañino	4 - Severo	1 - Insignificante	Extremo	Mitigar
20	Firewall(Asis)	Gerencia	Acceso a los sistemas de información o recursos tecnológicos por usuarios no autorizados.	Escalamiento de privilegios.	Fallas o ausencia de un procedimiento o proceso establecido para la revisión y/o supervisión de los derechos de acceso de los usuarios.	Baja	Baja	Baja	5 - Crítico	3 - Dañino	1 - Insignificante	1 - Insignificante	3 - Dañino	4 - Severo	1 - Insignificante	Extremo	Mitigar
21	Srv-Zeus	Gerencia	Acceso a los sistemas de información o recursos tecnológicos por usuarios no autorizados.	Escalamiento de privilegios.	Fallas o ausencia de un procedimiento o proceso establecido para la revisión y/o supervisión de los derechos de acceso de los usuarios.	Baja	Baja	Baja	5 - Crítico	3 - Dañino	1 - Insignificante	1 - Insignificante	3 - Dañino	4 - Severo	1 - Insignificante	Extremo	Mitigar
22	Firewall(Admi)	Gerencia	Acceso a los sistemas de información o recursos tecnológicos por usuarios no autorizados.	Escalamiento de privilegios.	Fallas o ausencia de un procedimiento o proceso establecido para la revisión y/o supervisión de los derechos de acceso de los usuarios.	Baja	Baja	Baja	5 - Crítico	3 - Dañino	1 - Insignificante	1 - Insignificante	3 - Dañino	4 - Severo	1 - Insignificante	Extremo	Mitigar

Ítem	Activos	Riesgos	Vulnerabilidades (Posible explotacion)	Plan de Accion Tecnico	Plan de Acceso	Control de Referencia ANEXO A ISO 27001:2013	Control de Referencia ANEXO A ISO 27032:2105	Tipo de Control	Nombre del colaborador y/o cargo responsable	Plazo (Días)	Fecha de Implementacion
1	HIS / Isalud	Ataques a sitios o aplicaciones web.	Parámetro incorrecto configurado	Implementar un WAF (Firewall de Aplicaciones Web) que garantice la proteccion contra el OWASP Top 10	Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen, evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	A.12.6.1 - Gestión de las vulnerabilidades técnicas	12.2 Controles a nivel de aplicación	Detectivo	Gerente Apoyo TI	180	1/09/2023
		Filtrado de información confidencial y/o sensible por acceso no autorizados y/o ataques de cookies.	El tráfico sensible sin proteccion	Implementar un WAF (Firewall de Aplicaciones Web) que garantice la proteccion contra el OWASP Top 10	Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen, evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	A.12.6.1 - Gestión de las vulnerabilidades técnicas	12.2 Controles a nivel de aplicación	Detectivo	Gerente Apoyo TI	180	1/09/2023
		Acceso a los sistemas de información e recursos tecnológicos por usuarios no autorizados.	Parámetro incorrecto configurado	Implementar un WAF (Firewall de Aplicaciones Web) que garantice la proteccion contra el OWASP Top 10	Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen, evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	A.12.6.1 - Gestión de las vulnerabilidades técnicas	12.2 Controles a nivel de aplicación	Detectivo	Gerente Apoyo TI	180	1/09/2023
2	Google Correo	Acceso a los sistemas de información e recursos tecnológicos por usuarios no autorizados.	La falta de identificación y autenticación de remitente y el receptor	Implementar una pasarela de correo electrónico segura con capacidades para proteger las herramientas colaborativas	La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	A.14.1.2 - Seguridad de servicios de las aplicaciones en redes publicas	12.4 Controles de Usuario	Preventivo	Gerente Apoyo TI	180	1/09/2023
3	Firewall(Asa)	Daño al centro de procesamiento de datos y/o servidores.	Red de energía inestable	Implementar dispositivos de seguridad perimetral en esquemas de alta disponibilidad donde se garantice la continuidad del servicio	Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	A.17.2.1 - Disponibilidad de instalaciones de procesamiento de información	12.3 Proteccion del servidor	Preventivo	Gerente Apoyo TI	180	1/09/2023
		Afectación de la continuidad de la operación por fallas en los sistemas de información	Arquitectura de red insegura	Implementar dispositivos de seguridad perimetral con funcionalidades de IDS, IPS con Anti DoS y DDoS que permita cerrar este tipo de ataques	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	A.13.1.1 - Controles de redes	12.2 Controles a nivel de aplicación	Detectivo	Gerente Apoyo TI	180	1/09/2023
		Fallas en los procesos tecnológicos.	Parámetro incorrecto configurado	Implementar dispositivos de seguridad Perimetral con los últimos niveles de firmware estables y seguros recomendados por el fabricante	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	A.13.1.1 - Controles de redes	12.3 Proteccion del servidor	Preventivo	Gerente Apoyo TI	180	1/09/2023
		Errores en la configuración y/o parametrización de la infraestructura tecnológica	Servicios innecesarios habilitados	Implementar dispositivos de seguridad perimetrales con funcionalidades de IDS y IPS que garantices los alertas tempras de un posible ataque	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	A.13.1.1 - Controles de redes	12.3 Proteccion del servidor	Detectivo	Gerente Apoyo TI	180	1/09/2023
		Afectación de la continuidad de la operación por fallas en los sistemas de información	Arquitectura de red insegura	Implementar dispositivos de seguridad perimetral con funcionalidades de IDS, IPS con Anti DoS y DDoS que permita cerrar este tipo de ataques	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	A.13.1.1 - Controles de redes	12.3 Proteccion del servidor	Detectivo	Gerente Apoyo TI	180	1/09/2023
4	Srv-Zeus	Daño al centro de procesamiento de datos y/o servidores.	Mantenimiento insuficiente / instalación deficiente de medios de almacenamiento	Implementar servidores con tecnologías de protección redundante (Energía, Almacenamiento)	Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	A.17.2.1 - Disponibilidad de instalaciones de procesamiento de información	12.3 Proteccion del servidor	Preventivo	Gerente Apoyo TI	180	1/09/2023
		Afectación de la continuidad de la operación por fallas en los sistemas de información	Arquitectura de red insegura	Implementar dispositivos de seguridad perimetral con funcionalidades de IDS, IPS con Anti DoS y DDoS que permita cerrar este tipo de ataques	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	A.13.1.1 - Controles de redes	12.3 Proteccion del servidor	Detectivo	Gerente Apoyo TI	180	1/09/2023
		Afectación de la continuidad de la operación por fallas en los sistemas de información	Arquitectura de red insegura	Implementar dispositivos de seguridad perimetral con funcionalidades de IDS, IPS con Anti DoS y DDoS que permita cerrar este tipo de ataques	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	A.13.1.1 - Controles de redes	12.3 Proteccion del servidor	Detectivo	Gerente Apoyo TI	180	1/09/2023
5	Firewall(Adm)	Daño al centro de procesamiento de datos y/o servidores.	Red de energía inestable	Implementar dispositivos de seguridad perimetral en esquemas de alta disponibilidad donde se garantice la continuidad del servicio	Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	A.17.2.1 - Disponibilidad de instalaciones de procesamiento de información	12.2 Controles a nivel de aplicación	Preventivo	Gerente Apoyo TI	180	1/09/2023
		Afectación de la continuidad de la operación por fallas en los sistemas de información	Arquitectura de red insegura	Implementar dispositivos de seguridad perimetral con funcionalidades de IDS, IPS con Anti DoS y DDoS que permita cerrar este tipo de ataques	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	A.13.1.1 - Controles de redes	12.3 Proteccion del servidor	Detectivo	Gerente Apoyo TI	180	1/09/2023
		Fallas en los procesos tecnológicos.	Parámetro incorrecto configurado	Implementar dispositivos de seguridad Perimetral con los últimos niveles de firmware estables y seguros recomendados por el fabricante	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	A.13.1.1 - Controles de redes	12.3 Proteccion del servidor	Preventivo	Gerente Apoyo TI	180	1/09/2023
		Errores en la configuración y/o parametrización de la infraestructura tecnológica	Servicios innecesarios habilitados	Implementar dispositivos de seguridad perimetrales con funcionalidades de IDS y IPS que garantices los alertas tempras de un posible ataque	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	A.13.1.1 - Controles de redes	12.3 Proteccion del servidor	Detectivo	Gerente Apoyo TI	180	1/09/2023
		Afectación de la continuidad de la operación por fallas en los sistemas de información	Arquitectura de red insegura	Implementar dispositivos de seguridad perimetral con funcionalidades de IDS, IPS con Anti DoS y DDoS que permita cerrar este tipo de ataques	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	A.13.1.1 - Controles de redes	12.3 Proteccion del servidor	Detectivo	Gerente Apoyo TI	180	1/09/2023
6	Google Correo	Daño al centro de procesamiento de datos y/o servidores.	Parámetro incorrecto configurado	Establecer acuerdos de nivel de servicio que garanticen la continuidad del servicio en caso de presentarse un incidente	Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación	A.15.1.3 - Cadena de suministro de tecnología de información y comunicación	12.2 Controles a nivel de aplicación	Preventivo	Gerente Apoyo TI	180	1/09/2023
		Ataques de virus.	Formación de seguridad insuficientes	Implementar una pasarela de correo electrónico segura que proteja las herramientas colaborativas de malware y ataques 0 Day	Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	A.12.2.1 - Controles contra códigos maliciosos	12.4 Controles del Usuario	Preventivo	Gerente Apoyo TI	180	1/09/2023
7	HIS / Isalud	Afectación de la continuidad de la operación por fallas en los sistemas de información	No hay pruebas de software o insuficiente	Implementar un WAF (Firewall de Aplicaciones Web) que garantice la proteccion contra el OWASP Top 10 y Balanceadores de Carga	La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	A.14.1.2 - Seguridad de servicios de las aplicaciones en redes publicas	12.2 Controles a nivel de aplicación	Detectivo	Gerente Apoyo TI	180	1/09/2023
8	Pit CC	Afectación de la continuidad de la operación por fallas en los sistemas de información	No hay pruebas de software o insuficiente	Implementar un WAF (Firewall de Aplicaciones Web) que garantice la proteccion contra el OWASP Top 10 y Balanceadores de Carga	La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	A.14.1.2 - Seguridad de servicios de las aplicaciones en redes publicas	12.2 Controles a nivel de aplicación	Detectivo	Gerente Apoyo TI	180	1/09/2023
9	Firewall(Adm)	Afectación de la continuidad de la operación por fallas en los sistemas de información	Fallas o ausencia en los planes de contrinuidad de negocio.	Implementar dispositivos de seguridad perimetral con esquemas de alta disponibilidad y con tecnologías de ZTNA	Se deben clasificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.	A.13.1.2 - Seguridad de los servicios de red	12.3 Proteccion del servidor	Preventivo	Gerente Apoyo TI	180	1/09/2023
10	Firewall(Adm)	Afectación de la continuidad de la operación por fallas en los sistemas de información	Fallas o ausencia en los planes de contrinuidad de negocio.	Implementar dispositivos de seguridad perimetral con esquemas de alta disponibilidad y con tecnologías de ZTNA	Se deben clasificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.	A.13.1.2 - Seguridad de los servicios de red	12.3 Proteccion del servidor	Preventivo	Gerente Apoyo TI	180	1/09/2023
11	Firewall(Adm)	Daño al centro de procesamiento de datos y/o servidores.	Ubicación en un área susceptible a las inundaciones	Se asume el riesgo porque no existe espacio locativo para acceder un nuevo cuarto tecnico que cumpla con los requisitos para evitar este tipo de riesgos	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros de entorno, y las posibilidades de acceso no autorizado.	A.11.2.1 - Ubicación y protección de los equipos	12.3 Proteccion del servidor		Gerente Apoyo TI	180	1/09/2023
		Afectación de la continuidad de la operación por fallas en los sistemas de información	Fallas o ausencia en los planes de contrinuidad de negocio.	Implementar dispositivos de seguridad perimetral con funcionalidades de IDS, IPS con Anti DoS y DDoS que permita cerrar este tipo de ataques	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	A.13.1.1 - Controles de redes	12.3 Proteccion del servidor	Detectivo	Gerente Apoyo TI	180	1/09/2023
12	Srv-Zeus	Daño al centro de procesamiento de datos y/o servidores.	Ubicación en un área susceptible a las inundaciones	Se asume el riesgo porque no existe espacio locativo para acceder un nuevo cuarto tecnico que cumpla con los requisitos para evitar este tipo de riesgos	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros de entorno, y las posibilidades de acceso no autorizado.	A.11.2.1 - Ubicación y protección de los equipos	12.3 Proteccion del servidor		Gerente Apoyo TI	180	1/09/2023
		Error en la calidad e integridad de la información	La falta de control de cambio de configuracion eficiente	Implementar un procedimientos para la gestion de cambios de TI	Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	A.12.1.2 - Gestión de cambios	12.3 Proteccion del servidor	Correctivo	Gerente Apoyo TI	180	1/09/2023
13	Firewall(Adm)	Daño al centro de procesamiento de datos y/o servidores.	Ubicación en un área susceptible a las inundaciones	Se asume el riesgo porque no existe espacio locativo para acceder un nuevo cuarto tecnico que cumpla con los requisitos para evitar este tipo de riesgos	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros de entorno, y las posibilidades de acceso no autorizado.	A.11.2.1 - Ubicación y protección de los equipos	12.3 Proteccion del servidor		Gerente Apoyo TI	180	1/09/2023
		Afectación de la continuidad de la operación por fallas en los sistemas de información	Fallas o ausencia en los planes de contrinuidad de negocio.	Implementar dispositivos de seguridad perimetral en IAA con funcionalidades de IDS, IPS con Anti DoS y DDoS que permita cerrar este tipo de ataques	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	A.13.1.1 - Controles de redes	12.3 Proteccion del servidor	Preventivo	Gerente Apoyo TI	180	1/09/2023
14	Firewall(Adm)	Daño al centro de procesamiento de datos y/o servidores.	La falta de proteccion física de los edificios, puertas y ventanas	Implementar sistemas de detección y extinción de incendios ó extintores de Co2	Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	A.17.2.1 - Disponibilidad de instalaciones de procesamiento de información	12.3 Proteccion del servidor	Preventivo	Gerente Apoyo TI	180	1/09/2023
15	Srv-Zeus	Daño al centro de procesamiento de datos y/o servidores.	La falta de proteccion física de los edificios, puertas y ventanas	Implementar sistemas de detección y extinción de incendios ó extintores de Co2	Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	A.17.2.1 - Disponibilidad de instalaciones de procesamiento de información	12.3 Proteccion del servidor	Preventivo	Gerente Apoyo TI	180	1/09/2023
16	Firewall(Adm)	Daño al centro de procesamiento de datos y/o servidores.	La falta de proteccion física de los edificios, puertas y ventanas	Implementar sistemas de detección y extinción de incendios ó extintores de Co2	Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	A.17.2.1 - Disponibilidad de instalaciones de procesamiento de información	12.3 Proteccion del servidor	Preventivo	Gerente Apoyo TI	180	1/09/2023
17	HIS / Isalud	Afectación de la continuidad de la operación por fallas en los sistemas de información	Arquitectura de red insegura	Implementar un WAF (Firewall de Aplicaciones Web) que garantice la proteccion contra el OWASP Top 10	La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	A.14.1.2 - Seguridad de servicios de las aplicaciones en redes publicas	12.2 Controles a nivel de aplicación	Detectivo	Gerente Apoyo TI	180	1/09/2023
		Afectación de la continuidad de la operación por fallas en los sistemas de información	Arquitectura de red insegura	Implementar un WAF (Firewall de Aplicaciones Web) que garantice la proteccion contra el OWASP Top 10	La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	A.14.1.2 - Seguridad de servicios de las aplicaciones en redes publicas	12.2 Controles a nivel de aplicación	Detectivo	Gerente Apoyo TI	180	1/09/2023
18	Pit CC	Afectación de la continuidad de la operación por fallas en los sistemas de información	Arquitectura de red insegura	Implementar un WAF (Firewall de Aplicaciones Web) que garantice la proteccion contra el OWASP Top 10	La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	A.14.1.2 - Seguridad de servicios de las aplicaciones en redes publicas	12.2 Controles a nivel de aplicación	Detectivo	Gerente Apoyo TI	180	1/09/2023
		Afectación de la continuidad de la operación por fallas en los sistemas de información	Arquitectura de red insegura	Implementar un WAF (Firewall de Aplicaciones Web) que garantice la proteccion contra el OWASP Top 10	La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	A.14.1.2 - Seguridad de servicios de las aplicaciones en redes publicas	12.2 Controles a nivel de aplicación	Detectivo	Gerente Apoyo TI	180	1/09/2023
19	Google Correo	Afectación de la continuidad de la operación por fallas en los sistemas de información	Arquitectura de red insegura	Implementar una pasarela de correo electrónico segura que proteja las herramientas colaborativas con funcionalidades de AntiSpam avanzado	La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	A.14.1.2 - Seguridad de servicios de las aplicaciones en redes publicas	12.2 Controles a nivel de aplicación	Preventivo	Gerente Apoyo TI	180	1/09/2023
		Afectación de la continuidad de la operación por fallas en los sistemas de información	Arquitectura de red insegura	Implementar una pasarela de correo electrónico segura que proteja las herramientas colaborativas con funcionalidades de AntiSpam avanzado	La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	A.14.1.2 - Seguridad de servicios de las aplicaciones en redes publicas	12.2 Controles a nivel de aplicación	Preventivo	Gerente Apoyo TI	180	1/09/2023
20	Firewall(Adm)	Acceso a los sistemas de información e recursos tecnológicos por usuarios no autorizados.	Fallas o ausencia de un procedimiento o proceso establecido para la revisión y/o supervisión de los derechos de acceso de los usuarios.	Implementar dispositivos de seguridad perimetral con funcionalidades de IDS y IPS que garantices los alertas tempras de un posible ataque	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	A.13.1.1 - Controles de redes	12.2 Controles a nivel de aplicación	Preventivo	Gerente Apoyo TI	180	1/09/2023
21	Srv-Zeus	Acceso a los sistemas de información e recursos tecnológicos por usuarios no autorizados.	Fallas o ausencia de un procedimiento o proceso establecido para la revisión y/o supervisión de los derechos de acceso de los usuarios.	Implementar dispositivos de seguridad perimetral con funcionalidades de IDS y IPS que garantices los alertas tempras de un posible ataque	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	A.13.1.1 - Controles de redes	12.2 Controles a nivel de aplicación	Preventivo	Gerente Apoyo TI	180	1/09/2023
22	Firewall(Adm)	Acceso a los sistemas de información e recursos tecnológicos por usuarios no autorizados.	Fallas o ausencia de un procedimiento o proceso establecido para la revisión y/o supervisión de los derechos de acceso de los usuarios.	Implementar dispositivos de seguridad perimetral con funcionalidades de IDS y IPS que garantices los alertas tempras de un posible ataque	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	A.13.1.1 - Controles de redes	12.2 Controles a nivel de aplicación	Preventivo	Gerente Apoyo TI	180	1/09/2023

Anexo G. Glosario de Términos

- **Activo de Información**

  Todo aquel elemento lógico o físico que conforme cualquiera de los sistemas de información de la organización.

- **Adware**

  Puede direccionar sus solicitudes de búsqueda a sitios web de publicidad y recopilar datos de marketing sobre usted en el proceso para que se muestren anuncios personalizados basados en su historial de búsqueda y compra.

- **Análisis de Riesgos**

  Proceso sistemático que permite identificar y determinar el impacto o grado de vulnerabilidad de los activos de la organización

- **API**

  Interfaz de programación de aplicaciones". En el contexto de las API, la palabra aplicación se refiere a cualquier software con una función distinta. La interfaz puede considerarse como un contrato de servicio entre dos aplicaciones.

- **BEC**

  El ataque al correo electrónico empresarial (BEC) es un tipo de ciberdelito donde el estafador utiliza el correo electrónico para engañar a alguien para que envíe dinero o revele información confidencial de la empresa.

- **DoS**

  Un ataque de denegación de servicio (DoS) es un tipo de ciberataque en el que un actor malicioso tiene como objetivo que un ordenador u otro dispositivo no esté disponible para los usuarios a los que va dirigido, interrumpiendo el funcionamiento normal del mismo.

- **DDoS**

  Un ataque DDoS, o ataque distribuido de denegación de servicio, es un tipo de ciberataque que intenta hacer que un sitio web o recurso de red no esté disponible colapsando con tráfico malintencionado para que no pueda funcionar correctamente.

- **DLP**

  Sistema de prevención de pérdida de datos es una solución que tiene como objetivo prevenir las fugas de información cuyo origen está dentro de la propia organización.

- **DMZ**

  Es una red local que se ubica entre la red interna de una organización y una red externa, generalmente en Internet. El objetivo de una DMZ es que las conexiones desde la red externa a la DMZ estén permitidas, mientras que en general las conexiones desde la DMZ hacia la red interna no están permitidas, esto hace que los equipos de la DMZ puedan dar servicios a la red externa, a la vez que protegen la red interna en el caso de que unos intrusos comprometan la seguridad de los equipos situados en la zona desmilitarizada.

- **EDR**

  Acrónimo en inglés de *Endpoint Detection Response*, es un sistema de protección de los equipos e infraestructuras de la empresa. Combina el antivirus tradicional junto con

herramientas de monitorización e inteligencia artificial para ofrecer una respuesta rápida y eficiente ante los riesgos y las amenazas más complejas.

- **ERP**

  El término ERP, o software ERP, se refiere a *Enterprise Resource Planning*, que significa “sistema de planificación de recursos empresariales”. El software ERP sirve para hacerse cargo de distintas operaciones internas de una organización.

- **Firewall (cortafuegos)**

  Un firewall es un elemento que sirve para filtrar las conexiones entrantes y salientes de una red, y que, junto a otros elementos, como el antivirus ofrece unas garantías de seguridad. Esto permite evitar ciberataques procedentes de Internet contra los dispositivos de la empresa, y que dichos dispositivos solamente establezcan las conexiones permitidas. De esta forma, se limitan los ataques procedentes, tanto de Internet, como de la red interna (*intranet*) de la empresa.

- **Firewall (NGFW- Firewall de nueva generación)**

  Este tipo de *firewall* está formado por diferentes elementos cada uno de los cuales ofrecerá una característica distinta, esto permite una mejor capacidad de procesamiento y ante la caída de uno de los servicios, el resto puede seguir funcionando con normalidad

- **Firewall Aplicaciones Web (WAF)**

  Es un tipo de firewall que supervisa, filtra o bloquea el tráfico HTTP y HTTPS hacia y desde una aplicación web. Se diferencia de un firewall normal en que puede filtrar el contenido de aplicaciones web específicas, mientras que un firewall de red protege el tráfico entre los servidores. Al inspeccionar el tráfico un WAF protege a las aplicaciones

web contra ataques como los de inyección SQL, XSS y falsificación de petición de sitios cruzados (CSRF).

- **Gusanos**

  Un gusano es un malware autónomo que puede propagarse y funcionar independientemente de otros archivos, mientras que un virus necesita un programa anfitrión para propagarse. Pueden ralentizar las redes informáticas al consumir ancho de banda y además afectar la eficacia del ordenador para procesar datos.

- **HIS**

  Sistema de información hospitalario o en salud que permite la gestión integrada de la información de los pacientes (citas, historia clínica, etc)

- **Historia Clínica Electrónica**

  La historia clínica es el registro obligatorio de las condiciones de salud del paciente y contiene los datos de los pacientes, el concepto de historia clínica electrónica y/o digital se ha usado indistintamente en Colombia para hacer referencia a un mismo proceso sobre un conjunto global y estructurado de información relacionado con los procesos asistenciales de un paciente en medios electrónicos.

- **IA Inteligencia Artificial**

  Es la combinación de algoritmos planteados con el propósito de crear máquinas que presenten las mismas capacidades que el ser humano.

- **IDS**

  Un sistema de detección de intrusos (Intrusion Detection System) es un sistema de supervisión que detecta actividades sospechosas y genera alertas al detectarlas

- **IPS**

  Un sistema de prevención de intrusos (Intrusion Prevention System) es una tecnología que vigila una red para detectar y bloquear cualquier actividad maliciosa que intente aprovechar la vulnerabilidad conocida.

- **MFA2**

  La autenticación multi factor (*multi factor authentication* o MFA) es una tecnología de seguridad que requiere múltiples métodos de autenticación de categorías independientes de credenciales para verificar la identidad de un usuario para un inicio de sesión u otra transacción

- **Phishing**

  En este ataque, mensajes que parecen legítimos manipulan a un usuario, haciéndole instalar un archivo malicioso, hacer clic en un enlace malicioso o divulgar información sensible como credenciales de acceso.

- **Postura Ciberseguridad**

  La postura de ciberseguridad se refiere a la estrategia y medidas que una organización adopta para proteger su infraestructura tecnológica de posibles amenazas cibernéticas.

- **Programas espía**

  Al igual que su nombre, el spyware es un virus informático que recopila información sobre una persona u organización sin su conocimiento expreso y puede enviar la información recopilada a un tercero sin el consentimiento del consumidor.

- **Ransomware**

  Software Malicioso (Malware) que infecta los dispositivos y cifra los archivos del sistema toma el control y secuestra la información, su propósito es la obtención de un rescate a través de bitcoins a cambio de eliminar la restricción

- **Sandboxing**

  Es una técnica de seguridad informática que se basa en la ejecución de programas o aplicaciones en un espacio virtual limitado, en el cual se pueden controlar todos los procesos sin que afecten al resto del equipo.

- **SD-WAN**

  La red de área extensa definida por el software (SD-WAN) es una tecnología transformadora que simplifica el control y la administración de la infraestructura de TI al proporcionar una arquitectura de WAN virtual que conecta de manera segura a los usuarios con sus aplicaciones.

- **SPAM**

  Es cualquier forma de comunicación no solicitada que se envía de forma masiva (correo electrónico masivo no solicitado, o UBE). Su forma más frecuente es un correo electrónico de publicidad enviado a un gran número de direcciones (correo electrónico de publicidad no solicitado

- **SSL**

  Es el acrónimo de Secure Sockets Layer (capa de sockets seguros), la tecnología estándar para mantener segura una conexión a Internet, así como para proteger cualquier información confidencial que se envía entre dos sistemas e impedir que los

delincuentes lean y modifiquen cualquier dato que se transfiera, incluida información que pudiera considerarse personal.

- **Sistema de información**

  Es un conjunto de componentes que interaccionan entre sí para alcanzar un fin determinado, el cual es satisfacer las necesidades de información de dicha organización

- **Troyano**

  Un troyano es un programa de puerta trasera que crea una vía de entrada para que usuarios malintencionados accedan al sistema informático utilizando lo que parece un programa real, pero que rápidamente resulta ser dañino. Un troyano puede eliminar archivos, activar otros programas maliciosos ocultos en la red informática, como un virus, y robar datos valiosos.

- **Virus**

  Un virus es un archivo malicioso descargable que ataca cambiando otros programas informáticos con su propio código. Una vez que se propaga, esos archivos quedan infectados y pueden propagarse de un ordenador a otro, y/o corromper o destruir datos de la red.

- **VPN**

  Una VPN no es una red física como tal, como podría ser la intranet corporativa, sino una red virtual de transmisión de la información sensible, de forma encapsulada y cifrada para evitar que pueda ser vista y utilizada por terceros.

Universidad®
Católica
de Manizales

VIGILADA MINEDUCACIÓN

Obra de Iglesia
de la Congregación

Hermanas de la Caridad
Dominicas de La Presentación
de la Santísima Virgen

Universidad Católica de Manizales
Carrera 23 # 60-63 Av. Santander / Manizales - Colombia
PBX (6)8 93 30 50 - www.ucm.edu.co