UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR

POSGRADOS

MAESTRÍA EN
SEGURIDAD DE LA INFORMACIÓN

RPC-SO-28-NO.669-2021

OPCIÓN DE TITULACIÓN:

PROYECTO DE TITULACIÓN CON COMPONENTES DE INVESTIGACIÓN APLICADA Y/O DE DESARROLLO

TEMA:

ELABORACIÓN DE UN PLAN DE CONTINUIDAD DEL NEGOCIO EN LA EMPRESA LA UNIÓN COMPAÑÍA NACIONAL DE SEGUROS

AUTOR:

JAIRO FERNANDO ALARCÓN LUNA

DIRECTOR:

JUAN CARLOS DOMÍNGUEZ AYALA

CUENCA – ECUADOR
2023

Autor:

Jairo Fernando Alarcón Luna
Ingeniero de Sistemas.
Candidato a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
jalarconl@est.ups.edu.ec

Dirigido por:

Juan Carlos Domínguez Ayala
Ingeniero de Sistemas.
Magister en Redes de Comunicaciones.
jdominguez@ups.edu.ec

DEDICATORIA

En primer lugar, dedicar la totalidad del trabajo a Dios ya que él es mi guía y con él en mi corazón puedo seguir sembrando y cosechando muchas cosas buenas.

También dedicar este trabajo a mi mamá Daisy, a mi papá Carlos, ya que son los pilares fundamentales en mi vida.

A mis hermanos Mauricio, Carlina y Matheo ya que de una u otra manera han colaborado directa o indirectamente en el desarrollo de mi trabajo

A mi novia Ana Belén ya que ha sido mi motivadora para seguir adelante con este proyecto y en los momentos difíciles me ha dado palabras de aliento para seguir luchando por mis objetivos.

A los que lastimosamente ya no están con vida a mi lado mi abuela Lida y mi abuelo Eliseo, pero sé que desde el cielo están guiando mis pasos.

A todos ellos y a las personas que indirectamente han hecho posible realizar este trabajo, Gracias.

AGRADECIMIENTO

Agradezco a Dios, a mis padres, a mis hermanos, a mi novia, a la familia de mi novia porque con sus consejos con su ayuda he podido seguir avanzando y especializándome en mi profesión.

Agradecer a la Universidad Politécnica Salesiana por brindar las herramientas necesarias para realizar el trabajo de titulación, al docente Juan Carlos Domínguez Ayala por su colaboración y recomendaciones a lo largo del desarrollo del programa de maestría.

Agradecer a mi jefe Fausto que me colaboró con sus conocimientos y consejos en el desarrollo de mi tesis.

Agradecer al director Alejandro Goldbaum de la Unión Compañía Nacional de Seguros por permitirme realizar el trabajo de titulación en la empresa.

Agradecer a Jonnathan Zhunio por ser un gran compañero de trabajos y proyectos de las materias de la maestría.

Agradecer en general a mis amigos que han sido parte del proceso de estudio.

Tabla de Contenido

Resumen 9
Abstract 10
1. Introducción 11
2. Determinación del Problema 12
3. Justificación 13
4. Objetivo General 14
5. Objetivos específicos 14
6. Marco teórico referencial 15
6.1 Descripción del contexto 15
6.1.1 ¿Quién es Seguros La Unión? 15
6.1.2 Ubicación geográfica 15
6.2 Plan de continuidad del negocio 16
2.1 Activo 16
6.3 Desastre 16
6.4 Amenaza 16
6.5 Vulnerabilidad 17
6.6 Riesgo 17
6.7 Identificación de activos 17
6.8 Almacenamiento de información 17
6.9 Seguridad con los proveedores 18
6.10 Norma ISO 22301 18
6.11 Magerit versión 3 19
6.12 Creación del plan de respuesta y recuperación 19
6.13 Descripción de la infraestructura 19
7. Detalle de la situación actual 21
7.1 Descripción 21
7.2 Descripción de los activos 27
7.3 Topología del Centro de Procesamiento de datos 37
8. Análisis de riesgos 38
8.1 Alcance 38

8.2 Parámetros 38
8.3 Valoración de activos 39
8.4 Riesgo intrínseco 43
8.5 Valoración de salvaguardas 49
8.6 Resumen riesgo final 50
8.7 Resultado diario por activo 58
9. Propuestas para continuidad del negocio 61
9.1 Rediseño de la red 61
9.1.1 Debilidades del diseño actual 61
9.1.2 Diseño de red propuesto 62
9.1.3 Implementación y cumplimiento de políticas de seguridad 64
9.1.4 Prácticas de seguridad de red recomendadas 65
9.1.5 Protección fundamental de red 67
9.1.6 Protección perimetral 72
9.1.7 Detalle de equipos a nivel de Seguridad Lógica 74
9.1.8 Nube de servidores públicos 77
9.2 Backup/Recovery Data Domain 79
9.2.1 Beneficios 79
9.2.2 Descripción de la solución 80
9.2.3 Esquema propuesto 81
9.3 Perfiles del personal de sistemas 82
10. Plan de respuesta y recuperación 83
10.1 Estrategias de recuperación 83
10.2 Tipos de estrategias 84
10.2.1 Backup 84
10.2.2 Suministro de energía alterna 84
10.2.3 Climatización 84
10.2.4 Control de acceso físico 85
10.2.5 Monitoreo en tiempo real 85
10.2.6 Rediseño de red 85
10.2.7 Seguridad perimetral 86
10.2.8 Sistema anti-spam 86
10.2.9 Extintor 86
10.3 Desarrollo de las estrategias 86
10.3.1 Backup 86

10.3.2 Suministro de energía alterna 87
10.3.3 Climatización 87
10.3.4 Control de acceso físico 87
10.3.5 Monitoreo en tiempo real 88
10.3.6 Rediseño de red 88
10.3.7 Seguridad perimetral 89
10.3.8 Sistema anti-spam 89
10.3.9 Extintor 90
11. PROBAR PLAN DE RESPUESTA Y RECUPERACION 90
11.1 Backup 90
11.2 Suministro de energía alterna 91
11.3 Climatización 92
11.4 Control de acceso físico 92
11.5 Monitoreo en tiempo real 93
11.6 Rediseño de red 94
11.7 Seguridad perimetral 94
11.8 Sistema Anti-spam 94
12. Políticas de seguridad 95
13. Monitorización y gestión 96
14. Conclusiones y recomendaciones 97
Referencias 99

ELABORACIÓN DE UN PLAN DE CONTINUIDAD DEL NEGOCIO EN LA EMPRESA LA UNIÓN COMPAÑÍA NACIONAL DE SEGUROS

AUTOR(ES):

JAIRO FERNANDO ALARCÓN LUNA

Resumen

En este trabajo se va a desarrollar la elaboración de un plan de continuidad del negocio enfocado a la infraestructura y almacenamiento de información del centro de procesamiento de datos para la empresa La Unión Compañía Nacional de Seguros domiciliada en la dirección Km. 5 ½ vía a la costa, Urbanización Los Cedros solares 1-2, ciudad de Guayaquil.

Es fundamental tener una correcta identificación y manejo de los riesgos, y a su vez definir y conocer los procedimientos a realizar para recuperar de manera eficiente y eficaz las operaciones del centro de procesamiento de datos ante cualquier amenaza que se materialice.

Como empresa de seguros debemos garantizar que nuestros servicios siempre estén disponibles para los clientes y es por tal motivo que los directores aprobaron la realización del presente trabajo que constará de 4 fases que son: trabajos iniciales (identificar los activos físicos que pertenecen a la compañía y de proveedores que se encuentran en el centro de procesamiento de datos, el almacenamiento de datos, identificar y priorizar las amenazas), análisis de impacto, crear plan de respuesta y recuperación, probar plan de ciberseguridad.

Para tener una garantía del correcto desarrollo de este trabajo se analizaron varios estándares y normas afines a la seguridad de la información.

Palabras clave:

Plan de continuidad, centro de procesamiento de datos, infraestructura, almacenamiento, amenazas, ciberseguridad, estándares, normas

ABSTRACT

In this work, the elaboration of a business continuity plan focused on the infrastructure and information storage of the data processing center for the company La Unión Compañía Nacional de Seguros domiciled at Km. 5 ½ via a la coast, Urbanization Los Cedros Solares 1-2, city of Guayaquil.

It is essential to have a correct identification and management of the risks, and in turn to define and know the procedures to be carried out to efficiently and effectively recover the operations of the data processing center in the face of any threat that materializes.

As an insurance company, we must guarantee that our services are always available to clients and it is for this reason that the directors approved the completion of this work, which will consist of 4 phases: initial work (identify the physical assets that belong to the company and providers that are in the data processing center, data storage, identify and prioritize threats), impact analysis, create response and recovery plan, test cybersecurity plan.

In order to have a guarantee of the correct development of this work, several standards and regulations related to information security were analyzed.

Keywords:

Continuity plan, data processing center, infrastructure, storage, threats, cybersecurity, standards, norm

1. INTRODUCCIÓN

Actualmente adentro de un centro de procesamiento de datos se implementan las tecnologías según las necesidades de las organizaciones, con ello se garantiza que el usuario tenga disponibilidad de los recursos y que la información se gestione de una manera correcta según las normativas.

Se debe considerar que estamos sujetos a vulnerabilidades, riesgos y amenazas que son desconocidas o conocidas, esto podría atentar contra el desarrollo y buen funcionamiento del centro de procesamientos de datos.

En su mayoría las tecnologías de información usadas actualmente cuentan con sistemas tolerantes a fallos, sin embargo, tenemos claro que existen amenazas y riesgos que podrían terminar en desastres, ya sean causados por errores informáticos, mala prácticas de los administradores, usuarios maliciosos, atacantes informáticos, de condición natural, es por eso que toda empresa debe contar con un plan de continuidad de negocio.

Dicho plan nos va a permitir que podamos identificar, eliminar o mitigar los riesgos que se encuentre en el centro de procesamiento de datos, y así reducir de manera correcta el tiempo de interrupción de los servicios.

El plan de continuidad del negocio del centro de procesamiento de datos va a contener información detallada y necesaria de los pasos y procedimientos que se debe seguir para restablecer los procesos críticos de la compañía.

En conclusión, vamos a definir en el primer capítulo a la compañía, su orientación, el estado actual del centro de procesamiento de datos, definición de términos a utilizar para la creación del plan de continuidad del negocio. En el segundo capítulo se encuentra detallado el plan de continuidad del negocio y los elementos que lo conforman. En el tercer capítulo se encuentra detallado el análisis de riesgo, definición de los roles y las responsabilidades.

2. Determinación del Problema

La empresa La Unión compañía Nacional de Seguros no cuenta con un plan de continuidad del negocio para el centro de procesamiento de datos, desempeñando el cargo de Asistente de Helpdesk he visualizado, verificado y notificado varios problemas en el centro de procesamiento de datos que podrían ser causa de una filtración o perdida de información por parte de los colaboradores ya que no es un área restringida con todas las condiciones que se requiere.

No se cuenta con un etiquetado correcto de cables utp, por tal motivo es difícil verificar el incidente rápidamente y gestionar la solución.

Los directores de la compañía reconocen la importancia de poseer un plan de continuidad del negocio de su centro de procesamiento de datos con la finalidad de estar preparados para responder y recuperarse ante cualquier incidente.

3. JUSTIFICACIÓN

La continuidad del negocio es fundamental en la compañía debido a la prioridad que se proporciona en los servicios que se ofrecen, a nivel financiero es muy positivo tener un plan como el que se va a desarrollar.

La compañía debe contar con ventaja competitiva en el mercado nacional e internacional, y con el desarrollo del plan de continuidad de negocio la tendrá, ya que tendremos disponibilidad aún después de la ocurrencia de un desastre eso aumentará la confianza de nuestros clientes.

Sobre los argumentos expuestos, y en base al trabajo que se va a realizar vamos a poder identificar y priorizar las amenazas actuales de la compañía con el fin de tener un plan de respuesta y recuperación de información.

4. Objetivo General

Elaborar un plan de ciberseguridad para garantizar la continuidad de las operaciones de la empresa La Unión Compañía Nacional de seguros

5. Objetivos específicos

Realizar la identificación de las amenazas actuales de la empresa, y definir el nivel de prioridad de cada una.

Realizar un análisis del impacto con la finalidad de entender como las operaciones son afectadas ante cualquier interrupción.

Crear un plan de respuesta y recuperación para cada uno de los elementos identificados.

Probar el plan de ciberseguridad y detallar los resultados obtenidos para establecer posibles actualizaciones.

6. Marco teórico referencial

6.1 Descripción del contexto

6.1.1 ¿Quién es Seguros La Unión?

La Unión Compañía Nacional de Seguros, fue fundada hace más de 75 años y es la primera compañía nacional de seguros en el Ecuador; desde sus inicios han sido pioneros en la actividad aseguradora privada introduciendo al mercado productos contemporáneos, brindando siempre lo mejor a nuestros clientes.

Algunos de los servicios que ofrecemos son: seguros personales, de propiedades, de garantías, de patrimonios, seguros masivos y seguimos innovando con la implementación de nuevos seguros para brindar excelencia a nuestros clientes.

6.1.2 Ubicación geográfica

El centro de procesamiento de datos se encuentra ubicado en la matriz de la compañía ubicada en el km 5.5 vía a la costa, urbanización los cedros solares 1 y 2.

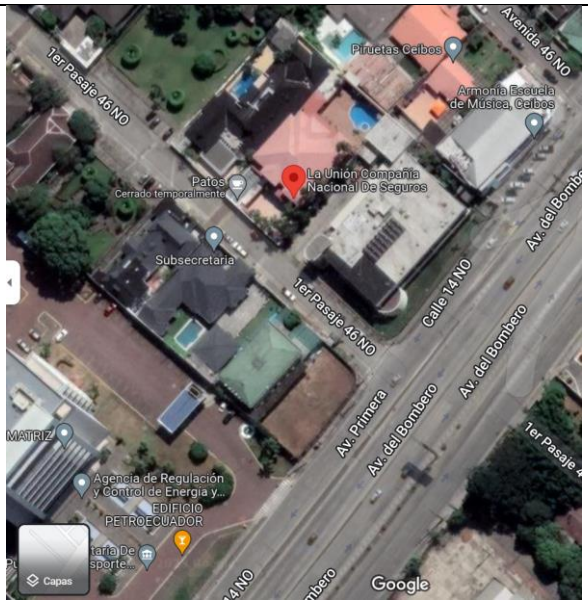


Figura 1: Visualización de la ubicación geográfica del centro de procesamiento de datos.
Fuente: Google Maps

6.2 Plan de continuidad del negocio

Según la investigación que se realizó muchos autores consideran un plan de continuidad del negocio como un conjunto de procedimientos o pasos a seguir antes, durante y después de un evento considerado como desastre; con la finalidad de que los servicios identificados como críticos se puedan restablecer en el menor tiempo posible de manera eficiente y eficaz para beneficio del usuario final.

2.1 Activo

Consideramos activo a todo lo que está adentro de nuestro centro de procesamiento de datos, ya sea a nivel físico o lógico. Ya que son de vital importancia para el correcto funcionamiento de las operaciones de la compañía, y estamos en la necesidad de protegerlos ante toda presencia de situaciones que pretendan poner en riesgo cualquier actividad que se ejecute normalmente.

6.3 Desastre

En el trabajo definiremos desastre a un evento que afecte directamente al centro de procesamiento de datos, para lo cual podemos definirlo en dos opciones que son los desastres naturales, los cuales no se van a poder predecir como se van a dar, cuando va a suceder o cual va a ser el impacto en nuestras operaciones críticas, también podemos nombrar a los desastres informáticos que son ataques lógicos y físicos en los cuales estamos expuestos según el software, hardware, los errores humanos, nivel de seguridad, etcétera.

6.4 Amenaza

Definimos a la amenaza como un evento o un factor que pueda ser capaz de afectar las operaciones del centro de procesamiento de datos, hay diversos tipos de amenazas como internas, externas, naturales, en el desarrollo del plan definiremos las amenazas presentes.

6.5 Vulnerabilidad

Según la investigación realizada definimos a la vulnerabilidad como una brecha de seguridad, que básicamente se presenta por una debilidad física o lógica que estaría presente en nuestro centro de procesamiento de datos, las cuales afectarían la seguridad, disponibilidad y la integridad de los datos, deteniendo la normalidad de nuestros servicios.

6.6 Riesgo

Definimos al riesgo como un evento que se ejecuta con cierto porcentaje de probabilidad, el cual afecta a las operaciones del centro de procesamiento de datos, pudiendo causar la perdida de datos o interrupción de servicios que se encuentran ejecutando, en ocasiones se conoce del riesgo y aunque se lo acepte no sabemos el momento en que se presente.

6.7 Identificación de activos

Se procederá a realizar un levantamiento de información formal de absolutamente todos los activos físicos que comprenden la infraestructura del centro de procesamiento de datos, detallando los equipos que son de propiedad de la compañía y los equipos que están prestando servicios por parte de los proveedores contratados por requerimientos del área de sistemas para un correcto funcionamiento empresarial.

6.8 Almacenamiento de información

Se especificará el o los equipos que estén funcionando como almacenamiento de información de los servidores y de los usuarios de la compañía, y se procederá a analizar su sistema de seguridad, la frecuencia con la que se realizan los respaldos, y si existe algún protocolo de verificación de los respaldos.

6.9 Seguridad con los proveedores

Se verificará la seguridad y confidencialidad que nos brindan los proveedores de servicios tecnológicos, en caso de ser necesario se solicitará vía correo electrónico documentación que certifique el cumplimiento de normas y protocolos de seguridad y respuesta a incidentes.

6.10 Norma ISO 22301

Esta norma nos brinda los principios, terminología y los procesos definir la gestión de la continuidad del negocio, es decir nos ayuda a tener buenas prácticas para gestionar el impacto que podemos llegar a tener por una interrupción.

Básicamente la norma nos ayuda a entender el tipo y la magnitud del impacto que como organización vamos a estar dispuestos a aceptar, mas no lograr una total mitigación del impacto.

Algunas de las ventajas de la norma son la tranquilidad que brindaría a la organización, protección a nivel monetario de la organización, resiliencia visible ya que los clientes van a notar que estamos preparados como organización a enfrentar cualquier interrupción de nuestros servicios, mejora la ciberseguridad ante cualquier ataque de un ciberdelincuente estaremos preparados para brindar nuestros servicios normalmente, y así tendremos la ventaja competitiva ya que responderemos eficazmente ante cualquier interrupción y no se van a ver afectados los servicios que ofrecemos.

EL sistema de gestión de continuidad del negocio tiene como base los principios fundamentales de otros sistemas de gestión que se basa en PHVA Planificar, Hacer, Verificar y Actuar.

6.11 MAGERIT VERSIÓN 3

Mediante la metodología de MAGERIT se procederá a realizar un análisis de gestión de riesgo con el fin de definir correctamente los activos, riesgos, salvaguardas, porcentajes, y lo que la compañía puede perder a nivel monetario si se llega a materializar algún incidente. Para lo cual vamos a especificar lo siguiente: definir parámetros, valoración de activos, justificación, riesgo intrínseco, salvaguardas, resumen del riesgo final, resultados por activos diario

6.12 CREACIÓN DEL PLAN DE RESPUESTA Y RECUPERACIÓN

Consiste en la elaboración de un informe ejecutivo que incluirá conclusiones y recomendaciones específicas, que constará de los siguiente: diseño de arquitectura de redes y seguridad informática, listado de elementos (equipos, programas y servicios) que se requieran para mejorar la plataforma tecnológica, plan de implementación de mejoras con sus recomendaciones específicas para gestionar, mitigar y/o eliminar los riesgos de seguridad de la información.

6.13 DESCRIPCIÓN DE LA INFRAESTRUCTURA

El centro de procesamiento de datos cuenta con un área aproximada de 8 metros cuadrados, a 30 centímetros del piso y a 50 centímetros del techo de la obra física, cuenta con piso y techo falso, sin seguridad física, y se encuentra ubicado en la misma oficina asignada al departamento de sistemas. En el área asignada se distribuyen los equipos en 2 rack los cuales detallaremos de manera general como están asignados:

El rack 1 consta de:

- 2 switch capa 2 marca D-Link
- 1 switch capa 2 TRENDnet

- Para administrar red inalámbrica tenemos: 1 switch Poe 16 puertos, 1 router tplink y 1 consola UBIQUITI.
- Nuestro proveedor principal de internet es Century Link y nos ofrece un enlace de fibra y un radio enlace, para el enlace de fibra tenemos 1 CISCO ISR 1100 Series, 1 ADVA FSP 150-GE114Pro y para el enlace respaldo tenemos 1 CISCO C1111-8P, ADVA FSP 150-GE114Pro y un CERAGON.
- Century también nos brinda el servicio de firewall, con un equipo FortiGate 60D, FORTINET.
- Nuestro proveedor secundario o de respaldo es Punto Net y nos ofrece un 1 Switch MikroTik RB2011Il-in, 1 Router Calix GigaHub y 1 Switching Power Supply Mean Well, adicional para que funcione correctamente con nuestra red interna tenemos un router Tp-link de nuestra propiedad.
- 3 regletas para rack

El rack 2 consta de:

- 2 switch CORE DELL N1524
- 1 servidor HP ProLiant DL160 G6
- 2 servidores DELL EMC PowerEdge R640
- 1 sistema de Almacenamiento DELL EMC PowerVault ME4012
- 1 QNAP TS-1232XU-RP
- 2 regletas para rack

Adicional adentro del área tenemos un sistema de energía ininterrumpida UPS E-T-N E SERIES DX 6KVA POWERWARE, un acondicionador de aire marca YORK como respaldo en caso de fallar el sistema de aire acondicionado central, una cámara de vigilancia monitoreando el ingreso al departamento de sistemas, pero no al área donde se encuentra en centro de procesamiento de datos, un sistema de protección contra incendios con un solo detector de humo.

PC clon Gigabyte H81M-H que aloja nuestro servidor de correo.

7. Detalle de la situación actual

El plan de continuidad del negocio para el centro de procesamiento de datos de la Unión Compañía Nacional de Seguros se enfoca en mantener las operaciones frente a cualquier evento que pueda causar la paralización de los servicios, teniendo en cuenta 3 factores fundamentales como el recurso humano que es responsable de la gestión de los activos, la infraestructura tecnológica que tenemos implementada, y los datos que se almacenan.

El plan de continuidad del negocio lo realizaremos a partir de las etapas presentadas a continuación:

- Identificación y descripción de los activos que forman parte de nuestro CPD.
- Realizar un análisis de riesgos.
- Definir los procesos, actividades y procedimientos según las normas y buenas prácticas para el plan de continuidad del negocio
- Identificación y definición de los roles y responsabilidades de las personas a cargo del centro de procesamiento de datos.
- Comprobar la funcionalidad del plan de continuidad del negocio.

7.1 Descripción

Actualmente nuestro departamento de sistemas no cuenta con políticas definidas para actuar en caso de una eventualidad, listado de activos, listado de amenazas, listado de riesgos, roles y responsabilidades en un documento, es por eso que se decidió por establecer un plan de continuidad del negocio para el centro de procesamiento de datos.

Se procedió a tomar fotografías del centro de procesamiento de datos y podemos evidenciar que no cumple con las buenas prácticas y recomendaciones que están establecidas en las normas, actualmente se encuentra en el siguiente estado:

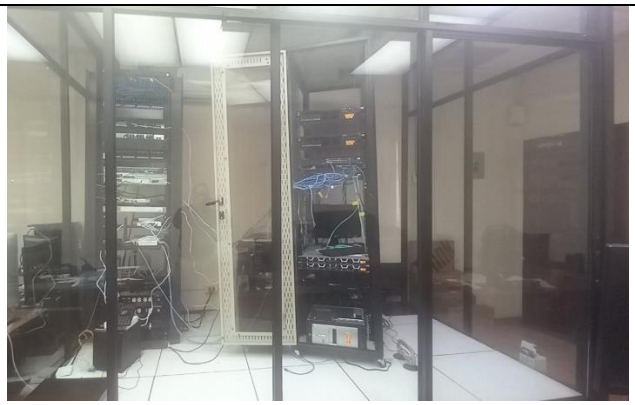


Figura 2: Fotografía del centro de procesamiento de datos.
Fuente: Autor

Figura 3: Fotografía del Acondicionador de aire.
Fuente: Autor

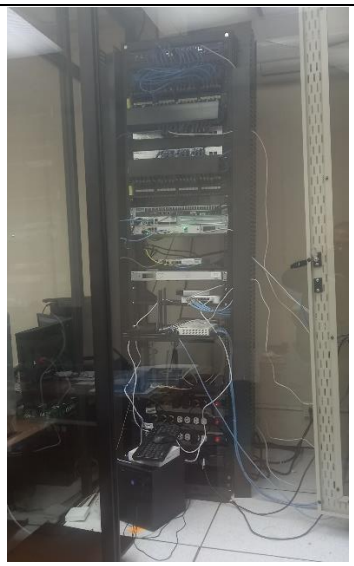


Figura 4: Fotografía del RACK 1.
Fuente: Autor

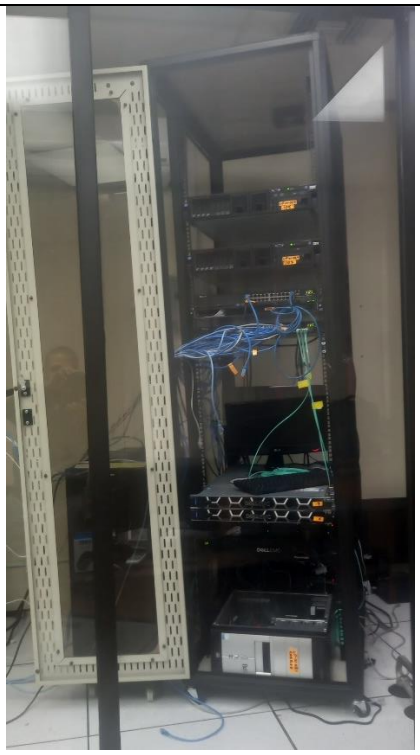


Figura 5: Fotografía del RACK 2.
Fuente: Autor

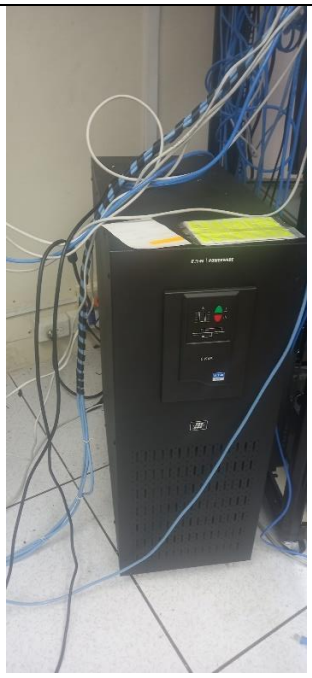


Figura 6: Fotografía del Sistema de Alimentación ininterrumpida UPS.
Fuente: Autor

Figura 7: Fotografía del servidor de correo
Fuente: Autor

Figura 8: Fotografía de la cámara de seguridad.
Fuente: Autor

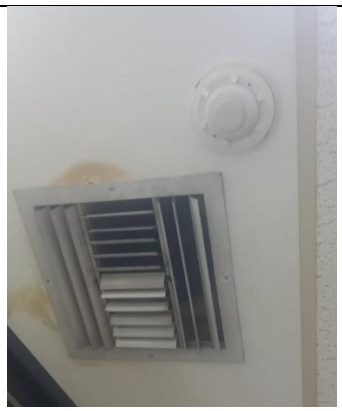


Figura 9: Fotografía detector de humo y rejilla de ventilación.
Fuente: Autor

Figura 10: Fotografía del techo en mal estado.
Fuente: Autor

Figura 11: Fotografía de conexiones eléctricas.
Fuente: Autor

Figura 13: Fotografía cableado de red usado en servidores.
Fuente: Autor

Figura 14: Fotografía de cableado de red desde el switch Core 1.
Fuente: Autor

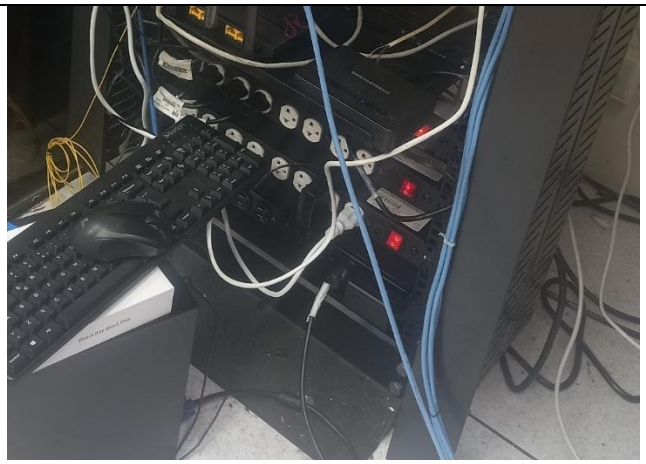


Figura 16: Fotografía de conexión eléctrica de RACK 1
Fuente: Autor

Figura 15: Fotografía de conexión eléctrica de RACK 2
Fuente: Autor

7.2 Descripción de los activos

En el centro de procesamiento de datos tenemos componentes de software y hardware los cuales están conectados para brindar los servicios de la compañía.

Para una buena distribución y caracterización de los activos vamos a proceder a definir por tablas la información del centro de procesamiento de datos con los siguientes nombres

- Tabla 1 Activos de personal
- Tabla 2 Activos tipo Hardware excluyendo servidores.
- Tabla 3 Activos tipo Software definidos como Base de datos.
- Tabla 4 Activos tipo Hardware definidos como servidores físicos.
- Tabla 5 Activos tipo Software definidos como servidores en la nube.
- Tabla 6 Activos tipo Software definidos como aplicaciones.
- Tabla 7 Activos tipo Software definidos como servidores virtuales.

En la siguiente tabla 1 vamos a definir al personal de sistemas que tiene acceso al centro de datos.

Tabla 1 Activos de personal

N.º	NOMBRE	FUNCIONES
1	Jefe de Sistemas	• Garantizar que todo lo relacionado a las herramientas informáticas estén en funcionamiento • Asegurar que toda la información esté respaldada • Coordinar que se realicen los requerimientos solicitados por las áreas de la empresa en materia de tecnología, inclusive cámaras de seguridad. • Revisar cambios en las Entidades de control en lo relacionado a las codificaciones y su

		funcionabilidad en las aplicaciones internas, y gestionar e instruir el correctivo. • Emitir o revisar estructuras y envío a las entidades de control • Anualmente gestionar y elaborar el presupuesto de área • Gestionar la solución de problemas de internet, telefonía móvil, radiofrecuencia etc., gestionando las soluciones con el proveedor correspondiente y en el menor tiempo posible para no afectar la operación. • Mantener las redes sociales actualizadas con información pertinente. • Dar soporte en cualquier área de la empresa de acuerdo a instrucciones gerenciales o de propietarios. • Cumplir con todas las responsabilidades inherentes al cargo relacionadas al sistema de gestión de calidad ISO 9001-2015.
2	Administrador de redes y base de datos	• Mantener el aplicativo Ensurance en correcto en funcionamiento, con las revisiones semanales de la base de datos • Crear usuarios según necesidades. • Realizar el respaldo semanal de la base de datos y el reporte correspondiente • Revisar con el jefe de Sistemas requerimientos de cambios en el sistema para ser aprobados • Monitorear la ejecución de los cambios en el sistema

		• Revisar diariamente el correcto funcionamiento de los servidores y solucionar problemas encontrados. • Monitorear el correcto servicio del internet • Realizar asistencia a los usuarios en el sistema • Realizar soporte a usuarios gerenciales y dueños de la empresa • Coordinar el mantenimiento preventivo y correctivo de la central telefónica • Dar mantenimiento del servidor de correos, eliminación y creación de usuarios • Realizar el ingreso de usuarios al reloj biométrico • Participar en implementaciones especiales entre sistemas • Realizar mantenimiento del sitio web • Emitir reporte mensual de vencimiento para el área de Emisiones • Emitir de reportes de facturación impaga mensual • Dar soporte en cualquier área de la empresa de acuerdo a instrucciones gerenciales o de propietarios. • Cumplir con todas las responsabilidades inherentes al cargo relacionadas al sistema de gestión de calidad ISO 9001-2015.
3	Asistente de Helpdesk	• Realizar el mantenimiento preventivo tanto de hardware como software de los equipos para asegurar la debida eficiencia. • Realizar inspección de equipos nuevos que ingresan a la empresa para verificar si es el adecuado y del que se solicitó.

		• Realizar el respaldo mensual de la información de todos los equipos de computación en la organización. • Coordinar el mantenimiento de equipos con proveedores externos y supervisar el mantenimiento correcto. • Recibir, atender y solucionar los requerimientos de los usuarios en coordinación con el jefe de sistemas. • Recibir, atender y solucionar los requerimientos de los usuarios de manera remota con sucursales de la empresa de acuerdo de las necesidades presentadas en el momento. • Visitar usuarios internos mensualmente para confirmar buen uso de equipos. • Analizar reportes de los equipos de la empresa de manera eventuales y dar soluciones. • Coordinar con proveedores de acuerdo con las necesidades que se presenten que se necesiten para cambios de equipos como impresoras, computadoras y diferentes aparatos • Revisar y ejecutar la instalación de equipos y actualización de Software y antivirus cada 3 o 6 meses. • Tener actualizado el stock, realizando las ordenes de pedido necesarias (tóner, teclados, actualización) • Comunicar situaciones críticas al jefe inmediato (caídas de servidor o danos graves de equipos)

		• Dar soporte en cualquier área de la empresa de acuerdo a instrucciones gerenciales o de propietarios. • Cumplir con todas las responsabilidades inherentes al cargo relacionadas al sistema de gestión de calidad ISO 9001-2015.

En la Tabla 2 se detalla los activos tipo hardware definidos para distribución de redes, monitoreo, telefonía internacional, ventilación que tenemos en el centro de procesamiento de datos

Tabla 2 Activos tipo Hardware excluyendo servidores.

N.º	**FABRICANTE**	**DESCRIPCIÓN**	**MODELO**	**PROPIO O PROVEEDOR**
1	TRENDnet	Switch capa 2	TEG-284WS	Propio
2	D-Link	Switch capa 2	DGS-1224T	Propio
3	D-Link	Switch capa 2	DGS-1224T	Propio
4	CERAGON	Radio Enlace	UNIT ACT	Proveedor
5	ADVA	Switch Radio Enlace	FSP 150-GE114Pro	Proveedor
6	CISCO	Router	C1111-8P	Proveedor
7	ADVA	Switch Fibra	FSP 150-GE114Pro	Proveedor
8	Fortinet	Firewall	FortiGate 60D	Proveedor
9	UniFi	Switch Network 16 PoE Lite Para Wireless Ubiquiti	USW-Lite-16-PoE	Propio
10	UniFi	Consola Wireless Ubiquiti	UCK-G2-PLUS	Propio
11	Tp-Link	DHCP Wireless	Archer C80	Propio
12	MikroTik	Switch – Enlace Secundario de Internet Punto Net	RB2011iL-IN	Proveedor

13	Calix GigaHub	Router - Enlace Secundario	813Gv2-1	Proveedor
14	Mean Well	Switching Power Supply	S-150-48	Proveedor
15	Tp-Link	Router para Enlace Secundario de Internet	TL-WR940N	Propio
16	E-T-N POWERWARE	UPS	E Series DK 6KVA	Propio
17	DELL	SWITCH CORE	N1524	Propio
18	DELL	SWITCH CORE	N1524	Propio
19	REGLETA	5 REGLETAS PARA RACK	TPL-19-4 MULTITOMA	Propio
20	CAT 5e, 6, 6a. y fibra óptica.	Cableado de datos	S/N	Propio
21	YORK	Split Aire Acondicionado	S/N	Propio
22	Central AC	Aire acondicionado centralizado.	S/N	Propio
23	Cable de corriente	Cableado eléctrico.	S/N	Propio

Tabla 3 Activos tipo Software definidos como Base de datos.

N.º	NOMBRE	MOTOR DE BASE DE DATOS	SERVIDOR	TIPO DE SERVIDOR	SISTEMA AL QUE SIRVE
1	dbmsun	Oracle 10g	oraclewin2008	virtual	Ensurance, emarine
2	helpdesk	MySQL	helpdesk	virtual	helpdesk

En la siguiente tabla 4 especificaremos los servidores físicos que forman parte del centro de procesamiento de datos, se hace énfasis que todos los equipos detallados son de propiedad de la Unión Compañía Nacional de Seguros

Tabla 4 Activos tipo Hardware definidos como servidores físicos.

N.º	FABRICANTE	MODELO	NOMBRE	PROCESADOR	MEMORIA RAM	DISCO DURO	SISTEMA OPERATIVO
1	HP	ProLiant DL160 G6	Veem Backup	Intel ® Xeon® E5620 @ 2.40 GHz	48 GB	240 GB	VMware ESXi, 6.7.0
2	DELL	PowerEdge R640	Server 6	16 CPUs x Intel(R) Xeon(R) Silver 4216 CPU @ 2.10GHz	128 GB	16 TB	VMware ESXi, 6.7.0
3	DELL	PowerEdge R640	Server 7	16 CPUs x Intel(R) Xeon(R) Silver 4216 CPU @ 2.10GHz	128 GB	16 TB	VMware ESXi, 6.7.0
4	QNAP	TS-1232XU-R	QNAP	Annapurna Labs Alpine AL324 Quad-core ARM Cortex-A57 CPU @ 1.70GHz	4 GB	64 TB	QTS 5.0.1.2194
5	DELL	ME 4012	PowerVault	Xeon® Broadwell-DE de 2 núcleos	S/I	19 TB	ME Storage Manager GT280R004-01
6	CLON	Gigabyte H81M-H	Mail Server	Core™ i7-4790 3.6GHz	16 GB	480 GB	Linux 2.6.32-754.e16.x86_64

En la siguiente tabla 5 especificaremos los servidores que se alojan en la nube que forman parte del centro de procesamiento de datos,

Tabla 5. Activos tipo Software definidos como servidores en la nube.

N.º	NOMBRE	SERVICIO	PROVEEDOR
1	ODOO	COMERCIALIZACION PRODUCTOS BANCA	TANDICORP
2	SURVIN	ENCUESTAS	TECSERVIN

En la siguiente tabla 6 especificaremos las aplicaciones que disponemos, cabe indicar que el departamento de sistemas no tiene un área de programadores y que todos los aplicativos son alquilados a proveedores de servicios.

Tabla 6 Activos tipo Software definidos como aplicaciones.

N.º	NOMBRE DEL SISTEMA	SOPORTE A	LENGUAJE DE PROGRAMACIÓN	COMPONENTES	BASE DE DATOS
1	Ensurance	Core Empresarial	Java	Base de datos, Tomcat, APP	Oracle 10G
2	Auto Nómina	Nómina	Visual Fox	Visual Fox	Visual Fox, Oracle 10G
3	Riesgos	Riesgos	PHP, JavaScript	Base de datos, Apache, APP	Oracle 10G
4	Surving	Encuestas	PHP, JavaScript	Base de datos, APP	Oracle 10G
5	Helpdesk	Mesa de ayuda	PHP, JavaScript	Base de datos, Apache, APP	MySQL

En la siguiente tabla 7 especificaremos los servidores virtuales que están en operación en nuestro centro de procesamiento de datos.

Tabla 7 Activos tipo Software definidos como servidores virtuales.

N.º	NOMBRE	AMBIENTE	SERVIDOR FÍSICO	CORE	MEMORIA RAM	SISTEMA OPERATIVO	DISCO DURO	SISTEMA
1	KASPERSKY	VMware vSphere	Host 1 Server 6	2 CORE	4 GB	Microsoft Windows Server 2019	204,09 GB	ANTIVIRUS
2	PLA-RIESGOS-220	VMware vSphere	Host 1 Server 6	2 CORE	4 GB	Microsoft Windows Server 2019	416,13 GB	CUMPLIMIENTO
3	RIESGOS-223	VMware vSphere	Host 1 Server 6	2 CORE	4 GB	Microsoft Windows Server 2019	408,8 GB	CUMPLIMIENTO
4	SERVIDOR 189 - MASIVOS	VMware vSphere	Host 1 Server 6	2 CORE	4 GB	Microsoft Windows 7 (64 bits)	2,78 TB	SEGUROS MASIVOS
5	SERVIDOR 221 - PCLAVADOS	VMware vSphere	Host 1 Server 6	8 CORE	12 GB	Microsoft Windows 7 (64 bits)	362,23 GB	CUMPLIMIENTO
6	SERVIDOR 229 PAGINA WEB	VMware vSphere	Host 1 Server 6	4 CORE	4 GB	Red Hat Enterprise Linux 5 (32 bits)	59,46 GB	PAGINA WEB
7	srvgyeavepr	VMware vSphere	Host 1 Server 6	4 CORE	4 GB	SUSE Linux Enterprise 11 (64 bits)	25,08 GB	AVAMAR
8	Tandicorp 82 clon	VMware vSphere	Host 1 Server 6	10 CORE	24 GB	Microsoft Windows 7 (64 bits)	148,02 GB	TANDICORP - ENSURANCE
9	Tandicorp-104-app-ensurance	VMware vSphere	Host 1 Server 6	6 CORE	16 GB	Ubuntu Linux (64 bits) 4.4.0	134,45 GB	TANDICORP - ENSURANCE
10	Tandicorp-23 server prueba	VMware vSphere	Host 1 Server 6	8 CORE	16 GB	Ubuntu Linux (64 bits) 4.4.0	116,09 GB	TANDICORP - ENSURANCE
11	Tandicorp-reports-2022-103	VMware vSphere	Host 1 Server 6	4 CORE	8 GB	Ubuntu Linux (64 bits) 4.4.0	108,1 GB	TANDICORP - ENSURANCE
12	Tandicorp-reports-crystal-agr-215	VMware vSphere	Host 1 Server 6	4 CORE	8 GB	Ubuntu Linux (64 bits) 4.4.0	108,08 GB	TANDICORP - ENSURANCE
13	Tanticorp-130-app-ensurance	VMware vSphere	Host 1 Server 6	12 CORE	16 GB	Ubuntu Linux (64 bits) 4.4.0	116,11 GB	TANDICORP - ENSURANCE
14	vCenter Converter	VMware vSphere	Host 1 Server 6	4 CORE	8 GB	Microsoft Windows Server 2019	40 GB	VMWARE
15	webs seguros la unión 2020 229	VMware vSphere	Host 1 Server 6	4 CORE	4 GB	CentOS 4/5 o posterior (64 bits)	223,51 GB	PAGINA WEB SERVER OFF
16	WS2016-NOMINA	VMware vSphere	Host 1 Server 6	2 CORE	8 GB	Microsoft Windows Server 2016	108,08 GB	NOMINA
17	WS2019-Veeam	VMware vSphere	Host 1 Server 6	2 CORE	8 GB	Microsoft Windows Server 2016	108,11 GB	VEEAM BACKUP

18	servidor200.seguroslaunion.com	VMware vSphere	Host 2 Server 7	2 CORE	4 GB	Microsoft Windows Server 2003 Standard (64 bits)	469,87 GB	SERVIDOR DE DOMINIO
19	fact-electronica-136	VMware vSphere	Host 2 Server 7	2 CORE	4 GB	Red Hat Enterprise Linux 5 (32 bits)	78,63 GB	FACTURACION ELECTRONICA
20	Tandicorp-104-app-OLD	VMware vSphere	Host 2 Server 7	6 CORE	16 GB	Ubuntu Linux (64 bits)	100,01 GB	TANDICORP - ENSURANCE - OFF
21	COMPARTIDOSSLU	VMware vSphere	Host 2 Server 7	4 CORE	8 GB	Microsoft Windows Server 2019	2,14 TB	DOCUMENTOS COMPARTIDOS
22	VMware vCenter Server Aplanche	VMware vSphere	Host 2 Server 7	2 CORE	10 GB	VMware vCenter Server Appliance 6.7.0.42000	107,26 GB	VMWARE
23	Tandicorp-120-emarine	VMware vSphere	Host 2 Server 7	8 CORE	32 GB	Ubuntu Linux (64 bits) 4.4.0	166,11 GB	TANDICORP - ENSURANCE
24	Tandicorp-214	VMware vSphere	Host 2 Server 7	12 CORE	16 GB	Ubuntu Linux (64 bits)	100 GB	TANDICORP - ENSURANCE - OFF
25	Tandicorp-27-nuevo	VMware vSphere	Host 2 Server 7	12 CORE	24 GB	Ubuntu Linux (64 bits) 4.4.0	124,1 GB	TANDICORP - ENSURANCE
26	Copia del 189 - 218	VMware vSphere	Host 2 Server 7	4 CORE	8 GB	Microsoft Windows 7 (64 bits)	167,58 GB	COPIA DE SERVER MASIVOS
27	Helpdesk	VMware vSphere	Host 2 Server 7	4 CORE	8 GB	CoreOS Linux (64 bits)	308,19 GB	MESA DE AYUDA
28	OracleWin2008	VMware vSphere	Host 2 Server 7	8 CORE	32 GB	Microsoft Windows Server 2008 R2 (64 bits)	1,64 TB	BASE DE DATOS
29	Oracle Test	VMware vSphere	Host 2 Server 7	4 CORE	16 GB	Microsoft Windows Server 2008 R2 (64 bits)	1,48 TB	BASE DE DATOS
30	Tandicorp-mes-anterior	VMware vSphere	Host 2 Server 7	12 CORE	16 GB	Ubuntu Linux (64 bits) 4.4.0	134,1 GB	TANDICORP - ENSURANCE
31	CrystalClear	VMware vSphere	Host 2 Server 7	2 CORE	8 GB	Microsoft Windows 10 (64 bits)	100 GB	TANDICORP - ENSURANCE - OFF

7.3 Topología del Centro de Procesamiento de datos

Actualmente el centro de procesamiento de datos se encuentra conectado sin las respectivas recomendaciones de las buenas prácticas, podemos evidenciar que todo el tráfico de datos pasa por el switch Core principal dejando por fuera a nuestro Fortinet firewall.

Adicional no contamos con una distribución de red adecuada, ya que no se administra la red con asignación de VLANs; toda nuestra red está asignada al segmento 192.168.1.x es por eso el motivo que de nuestra red colapse en ocasiones.

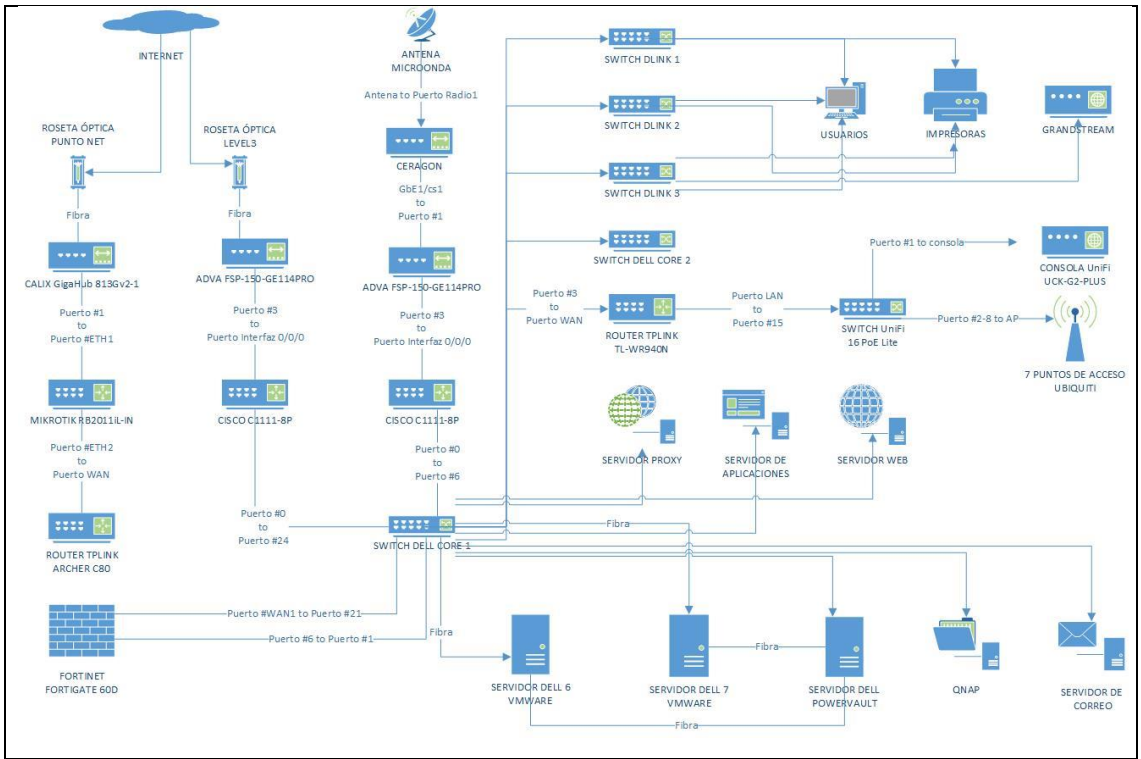


Figura 16: Topología del centro de procesamiento de datos
Fuente: Autor

8. Análisis de riesgos

Para el análisis de riesgos usaremos Magerit para plantear los riesgos en valores económicos y poder obtener una mayor apertura al momento de conversar con la gerencia sobre los plantes que debemos aplicar.

8.1 Alcance

El alcance del análisis de riesgos es definir los parámetros de evaluación, definir los activos, agruparlos y establecer su valoración considerando valor de reposición, uso, configuración y pérdida, definir las salvaguardas y calcular el riesgo inicial y el riesgo final aplicando las medidas establecidas para el centro de procesamiento de datos de la Unión Compañía Nacional de Seguros.

8.2 Parámetros

A continuación, se detallarán los parámetros que utilizaremos para nuestro análisis.

Tabla 8 de valoración de los activos

Valoración de los activos

Nivel	Abreviatura	Valor
Muy alto	MA	500000 $
Alto	A	100000 $
Medio	M	30000 $
Bajo	B	3000 $
Muy bajo	MB	500 $

Tabla 9 Calificación de la vulnerabilidad

Clasificación de la vulnerabilidad

Nivel	Abreviatura	Valor	Descripción
Extremadamente frecuente	EF	0,9973	1 vez cada día
Muy frecuente	MF	0,1425	1 vez cada semana
Frecuente	F	0,0329	1 vez cada mes
Frecuencia normal	FN	0,0055	1 vez cada 6 meses
Poco frecuente	PF	0,0027	1 vez al año
Extremadamente poco frecuente	EPF	0,0001	1 vez cada 20 años

Tabla 10 Valoración de impacto

Valoración del impacto

Nivel	Abreviatura	Valor
Crítico	MA	90%
Alto	A	75%
Medio	M	50%
Bajo	B	20%

Tabla 11 Disminución del impacto y de la vulnerabilidad

Disminución del impacto y de la vulnerabilidad

Nivel	Abreviatura	Valor
Alta	A	90%
Media	M	60
Baja	B	30
Nula	N	0%

Tabla 12 Nivel de riesgo

Nivel de riesgo

Nivel	Abreviatura	Valor
Muy alto	MA	300000 $
Alto	A	20000 $
Medio	MA	10000 $
Bajo	B	500 $
Muy bajo	N	100 $

.

8.3 Valoración de activos

Definimos un total de 65 activos en nuestro centro de procesamiento de datos, agrupados por categorías como datos, servicios, software, hardware, red de comunicaciones, soportes de información, equipo auxiliar, instalación y personal.

En la tabla tenemos el valor total del archivo según la importancia en la compañía, ese valor resulta de la suma de valores de reposición, uso, configuración y pérdida.

Resaltamos los activos que están en el rango de Alto con el color naranja y Muy Alto con el color rojo.

Tabla 13 Lista de activos del centro de procesamiento de datos.

N.º	Código	GRUPO	Descripción	Valoración cuantitativa	Valoración cualitativa
1	D-1	[D] Datos/Información	Respaldo de información de usuarios	$ 100.000,00	A
2	D-2	[D] Datos/Información	Respaldo de servidores virtuales	$ 500.000,00	MA
3	D-3	[D] Datos/Información	Base de datos del sistema Ensurance	$ 500.000,00	MA
4	D-4	[D] Datos/Información	Base de datos del sistema Auto nómina	$ 100.000,00	A
5	D-5	[D] Datos/Información	Base de datos del sistema Helpdesk	$ 3.000,00	B
6	D-6	[D] Datos/Información	Base de datos del sistema Riesgo	$ 30.000,00	M
7	D-7	[D] Datos/Información	Base de datos del sistema Surving	$ 30.000,00	M
8	D-8	[D] Datos/Información	Datos de servidor compartido	$ 500.000,00	MA
9	S-1	[S] Servicios	servicio de correo electrónico	$ 500.000,00	MA
10	S-2	[S] Servicios	almacenamiento de ficheros NetBak	$ 500.000,00	MA
11	S-3	[S] Servicios	servicio página web	$ 100.000,00	A
12	S-4	[S] Servicios	VMware v Sphere	$ 500.000,00	MA
13	S-5	[S] Servicios	Servicio emarine	$ 30.000,00	M
14	SW-1	[SW] Software	Servidor de correo electrónico	$ 500.000,00	MA
15	SW-2	[SW] Software	Servidor Ensurance	$ 30.000,00	M
16	SW-3	[SW] Software	Servidor de página web	$ 30.000,00	M
17	SW-4	[SW] Software	Servidor de Riesgo	$ 30.000,00	M
18	SW-5	[SW] Software	Servidor de encuesta Surving	$ 30.000,00	M
19	SW-6	[SW] Software	Servidor Auto Nómina	$ 30.000,00	M
20	SW-7	[SW] Software	Servidor de Helpdesk	$ 30.000,00	M
21	SW-8	[SW] Software	Servidor de Antivirus	$ 30.000,00	M
22	SW-9	[SW] Software	Gestor de VM VMware vSphere	$ 500.000,00	MA

23	SW-10	[SW] Software	Veem Backup	$ 500.000,00	MA
24	HW-1	[HW] Hardware	Switch capa 2 TRENDnet	$ 30.000,00	M
25	HW-2	[HW] Hardware	Switch capa 2 D-Link	$ 30.000,00	M
26	HW-3	[HW] Hardware	Switch capa 2 D-Link	$ 30.000,00	M
27	HW-4	[HW] Hardware	CERAGON Radio Enlace	$ 3.000,00	B
28	HW-5	[HW] Hardware	Switch ADVA FSP 150-GE114Pro	$ 30.000,00	M
29	HW-6	[HW] Hardware	Switch ADVA FSP 150-GE114Pro	$ 3.000,00	B
30	HW-7	[HW] Hardware	Router Cisco C1111-8P	$ 30.000,00	M
31	HW-8	[HW] Hardware	Router Cisco C1111-8P	$ 3.000,00	B
32	HW-9	[HW] Hardware	Cortafuegos Fortinet FortiGate 60D	$ 100.000,00	A
33	HW-10	[HW] Hardware	Switch UniFi USW-Lite-16-PoE	$ 3.000,00	B
34	HW-11	[HW] Hardware	Consola UniFi UCK-G2-PLUS	$ 3.000,00	B
35	HW-12	[HW] Hardware	Router Tp-Link Archer C80	$ 3.000,00	B
36	HW-13	[HW] Hardware	Router Tp-Link	$ 3.000,00	B
37	HW-14	[HW] Hardware	Switch MikroTik RB2011iL-IN	$ 500,00	MB
38	HW-15	[HW] Hardware	Router Calix GigaHub	$ 500,00	MB
39	HW-16	[HW] Hardware	Switching Power Supply Mean Well	$ 500,00	MB
40	HW-17	[HW] Hardware	Switch capa 3 DELL N1524	$ 30.000,00	M
41	HW-18	[HW] Hardware	Switch capa 3 DELL N1524	$ 3.000,00	B
42	HW-19	[HW] Hardware	HP ProLiant DL160 G6	$ 100.000,00	A
43	HW-20	[HW] Hardware	DELL PowerEdge R640	$ 100.000,00	A
44	HW-21	[HW] Hardware	DELL PowerEdge R640	$ 100.000,00	A
45	HW-22	[HW] Hardware	QNAP TS-1232XU-R	$ 100.000,00	A

46	HW-23	[HW] Hardware	DELL ME 4012	$ 100.000,00	A
47	HW-24	[HW] Hardware	CLON Gigabyte H81M-H	$ 100.000,00	A
48	COM-1	[COM] Redes de Comunicaciones	Red Principal de Internet Level3	$ 30.000,00	M
49	COM-2	[COM] Redes de Comunicaciones	Red de comunicaciones radio enlace	$ 30.000,00	M
50	COM-3	[COM] Redes de Comunicaciones	Red Secundaria de Internet Punto Net	$ 30.000,00	M
51	COM-4	[COM] Redes de Comunicaciones	Red inalámbrica	$ 30.000,00	M
52	MEDIA-1	[MEDIA] Soportes de Información	Almacenamiento en red (SAN)	$ 100.000,00	A
53	MEDIA-2	[MEDIA] Soportes de Información	Discos virtuales (vdisk)	$ 30.000,00	M
54	AUX-1	[AUX] Equipo auxiliar	Cableado de datos	$ 100.000,00	A
55	AUX-2	[AUX] Equipo auxiliar	Cableado eléctrico	$ 30.000,00	M
56	AUX-3	[AUX] Equipo auxiliar	Fibra óptica	$ 30.000,00	M
57	AUX-4	[AUX] Equipo auxiliar	Aire acondicionado York 18000 BTU	$ 30.000,00	M
58	AUX-5	[AUX] Equipo auxiliar	Aire acondicionado centralizado	$ 30.000,00	M
59	AUX-6	[AUX] Equipo auxiliar	Sistema de alimentación ininterrumpida E-T-N POWERWARE	$ 30.000,00	M
60	AUX-7	[AUX] Equipo auxiliar	Rack de comunicaciones	$ 30.000,00	M
61	AUX-8	[AUX] Equipo auxiliar	Rack de servidores	$ 30.000,00	M
62	L-1	[L] Instalaciones	Cuarto del centro de procesamiento de datos	$ 30.000,00	M
63	P-1	[P] Personal	Jefe de Sistemas	$ 30.000,00	M
64	P-2	[P] Personal	Administrador de redes y base de datos	$ 3.000,00	B
65	P-3	[P] Personal	Asistente de Helpdesk	$ 30.000,00	M

.

8.4 Riesgo intrínseco

Se realiza el cálculo de riesgo intrínseco para determinar el riesgo actual de los activos.

Tabla 14 Detalle diario y anual del riesgo intrínseco por amenaza.

Riesgo intrínseco por Amenaza			RIESGO INTRÍNSECO DIARIO POR AMENAZA	RIESGO INTRÍNSECO ANUAL POR AMENAZA
N.º	Código	AMENAZA		
1	AM-01	Incendio	$537,02	$196.012,30
2	AM-02	Desastre natural	$537,02	$196.012,30
3	AM-03	Fallo / avería de Hardware (físico)	$107,15	$39.109,75
4	AM-04	Fallo de servicios de comunicaciones	$224,25	$81.851,25
5	AM-05	Avería climatización	$1.278,00	$466.470,00
6	AM-06	Perdida de suministro de energía	$6.119,82	$2.233.734,30
7	AM-07	Robo personal interno	$474,17	$173.070,23
8	AM-08	Robo personas externas	$12.802,46	$4.672.896,08
9	AM-09	Ataque informático	$16.990,83	$6.201.652,95
10	AM-10	Vulnerabilidad de programas	$12.400,29	$4.526.105,85
11	AM-11	Indisponibilidad lógica	$12.975,39	$4.736.017,35
12	AM-12	Indisponibilidad personal	$147,42	$53.808,30
13	AM-13	Errores humanos	$599,54	$218.830,28
14	AM-14	Errores de configuración	$599,54	$218.830,28
15	AM-15	Caída del sistema por agotamiento de recursos	$7.449,30	$2.718.994,50
16	AM-16	Fuga de información	$459,27	$167.633,55
17	AM-17	Acceso no autorizado	$19.663,16	$7.177.051,58
18	AM-18	Fallo en copias	$1.458,00	$532.170,00
19	AM-19	Manipulación de equipos	$6.946,97	$2.535.642,23
20	AM-20	Modificación de la información	$12.400,29	$4.526.105,85
21	AM-21	Errores de mantenimiento físico / actualización de programas	$19.873,80	$7.253.937,00
22	AM-22	Difusión de software dañino	$15.206,94	$5.550.533,10
23	AM-23	Destrucción de información	$459,27	$167.633,55
24	AM-24	Pérdida de información	$12.400,29	$4.526.105,85

Tabla 15 Detalle diario y anual del riesgo intrínseco por activo

Riesgo intrínseco por activo			
	AC-01	AC-02	AC-03
	Respaldo de información de usuarios	Respaldo de servidores virtuales	Base de datos del sistema Ensurance
Riesgo intrínseco diario por activo	$3.186,02	$11.250,00	$13.725,00
Riesgo intrínseco anual por activo	$1.162.897,19	$4.106.250,00	$5.009.625,00
	AC-04	AC-05	AC-06
	Base de datos del sistema Auto nomina	Base de datos del sistema Helpdesk	Base de datos del sistema de Riesgo
Riesgo intrínseco diario por activo	$2.745,00	$74,64	$747,00
Riesgo intrínseco anual por activo	$1.001.925,00	$27.243,60	$272.655,00
	AC-07	AC-08	AC-09
	Base de datos del sistema Surving	Datos de servidor compartido	servicio de correo electrónico
Riesgo intrínseco diario por activo	$746,40	$12.510,00	$14.940,00
Riesgo intrínseco anual por activo	$272.436,00	$4.566.150,00	$5.453.100,00
	AC-10	AC-11	AC-12
	almacenamiento de ficheros NetBak	servicio página web	VMware vSphere
Riesgo intrínseco diario por activo	$14.940,00	$2.544,00	$13.725,00
Riesgo intrínseco anual por activo	$5.453.100,00	$928.560,00	$5.009.625,00
	AC-13	AC-14	AC-15

	Servicio emarine	Servidor de correo electrónico	Servidor Ensurance
Riesgo intrínseco diario por activo	$763,20	$13.725,00	$1.635,30
Riesgo intrínseco anual por activo	$278.568,00	$5.009.625,00	$596.884,50
	AC-16	AC-17	AC-18
	Servidor de página web	Servidor de Riesgo	Servidor de encuesta Surving
Riesgo intrínseco diario por activo	$747,00	$747,00	$746,40
Riesgo intrínseco anual por activo	$272.655,00	$272.655,00	$272.436,00
	AC-19	AC-20	AC-21
	Servidor Auto Nomina	Servidor de Helpdesk	Servidor de Antivirus
Riesgo intrínseco diario por activo	$750,60	$746,40	$670,80
Riesgo intrínseco anual por activo	$273.969,00	$272.436,00	$244.842,00
	AC-22	AC-23	AC-24
	Gestor de VM VMware vSphere	Veem Backup	Switch capa 2 TRENDnet
Riesgo intrínseco diario por activo	$9.990,00	$9.990,00	$417,60
Riesgo intrínseco anual por activo	$3.646.350,00	$3.646.350,00	$152.424,00
	AC-25	AC-26	AC-27
	Switch capa 2 D-Link	Switch capa 2 D-Link	CERAGON Radio Enlace
Riesgo intrínseco diario por activo	$417,60	$417,60	$39,33
Riesgo intrínseco	$152.424,00	$152.424,00	$14.355,45

anual por activo			
	AC-28	AC-29	AC-30
	Switch ADVA FSP 150-GE114Pro	Switch ADVA FSP 150-GE114Pro	Router Cisco C1111-8P
Riesgo intrínseco diario por activo	$452,70	$39,33	$452,70
Riesgo intrínseco anual por activo	$165.235,50	$14.355,45	$165.235,50
	AC-31	AC-32	AC-33
	Router Cisco C1111-8P	Cortafuegos Fortinet FortiGate 60D	Switch UniFi USW-Lite -16-PoE
Riesgo intrínseco diario por activo	$39,33	$1.513,00	$54,27
Riesgo intrínseco anual por activo	$14.355,45	$552.245,00	$19.808,55
	AC-34	AC-35	AC-36
	Consola UniFi UCK-G2-PLUS	Router Tp-Link Archer C80	Router Tp-Link
Riesgo intrínseco diario por activo	$39,33	$39,33	$39,33
Riesgo intrínseco anual por activo	$14.355,45	$14.355,45	$14.355,45
	AC-37	AC-38	AC-39
	Switch MikroTik RB2011iL-IN	Router Calix GigaHub	Switching Power Supply Mean Well
Riesgo intrínseco diario por activo	$6,56	$9,43	$4,08
Riesgo intrínseco anual por activo	$2.392,58	$3.440,89	$1.489,20
	AC-40	AC-41	AC-42
	Switch capa 3 DELL N1524	Switch capa 3 DELL N1524	HP ProLiant DL160 G6

Riesgo intrínseco diario por activo	$454,20	$39,33	$1.757,00
Riesgo intrínseco anual por activo	$165.783,00	$14.355,45	$641.305,00
	AC-43	AC-44	AC-45
	DELL PowerEdge R640	DELL PowerEdge R640	QNAP TS-1232XU-R
Riesgo intrínseco diario por activo	$2.007,00	$2.007,00	$2.007,00
Riesgo intrínseco anual por activo	$732.555,00	$732.555,00	$732.555,00
	AC-46	AC-47	AC-48
	DELL ME 4012	CLON Gigabyte H81M-H	Red Principal de Internet Level3
Riesgo intrínseco diario por activo	$2.007,00	$2.007,00	$586,05
Riesgo intrínseco anual por activo	$732.555,00	$732.555,00	$213.908,25
	AC-49	AC-50	AC-51
	Red de comunicaciones radio enlace	Red Secundaria de Internet Punto Net	Red inalámbrica
Riesgo intrínseco diario por activo	$428,40	$358,20	$546,00
Riesgo intrínseco anual por activo	$156.366,00	$130.743,00	$199.290,00
	AC-52	AC-53	AC-54
	Almacenamiento en red (SAN)	Discos virtuales (vdisk)	Cableado de datos
Riesgo intrínseco diario por activo	$1.323,00	$307,80	$783,00
Riesgo intrínseco	$482.895,00	$112.347,00	$285.795,00

anual por activo			
	AC-55	AC-56	AC-57
	Cableado eléctrico	Fibra óptica	Aire acondicionado York 18000 BTU
Riesgo intrínseco diario por activo	$234,90	$234,90	$199,35
Riesgo intrínseco anual por activo	$85.738,50	$85.738,50	$72.762,75
	AC-58	AC-59	AC-60
	Aire acondicionado centralizado	Sistema de alimentación ininterrumpida E-T-N POWERWARE	Rack de comunicaciones
Riesgo intrínseco diario por activo	$278,10	$230,25	$7,20
Riesgo intrínseco anual por activo	$101.506,50	$84.041,25	$2.628,00
	AC-61	AC-62	AC-63
	Rack de servidores	Cuarto del centro de procesamiento de datos	Jefe de Sistemas
Riesgo intrínseco diario por activo	$7,20	$7.710,75	$966,60
Riesgo intrínseco anual por activo	$2.628,00	$2.814.423,75	$352.809,00
	AC-64	AC-65	
	Administrador de redes y base de datos	Asistente de Helpdesk	
Riesgo intrínseco diario por activo	$9,45	$966,60	
Riesgo intrínseco anual por activo	$3.449,25	$352.809,00	

8.5 Valoración de salvaguardas

Se realiza la valoración de las salvaguardas con la finalidad de verificar el costo de su adquisición e implementación.

Tabla 16 Detalle del costo de las salvaguardas a implementar y activos que afectan

N.º	Código	Descripción	Valoración cuantitativa	ACTIVOS A IMPPLEMENTAR
1	SG-001	Extintor	$100,00	D-S-SW-HW-COM-MEDIA-AUX-L
2	SG-002	Copia de Seguridad en nube	$20.000,00	D-S-SW
3	SG-003	Guardar respaldo de información en caja de seguridad	$100,00	D-S-SW
4	SG-004	Copia de seguridad en equipo alterno	$0,00	D-S-SW
5	SG-005	Cifrado de la información	$2.000,00	D-S-SW
6	SG-006	Administración de perfiles de usuarios	$0,00	D-S-SW-P
7	SG-007	Anti-spam Contratado con Cirion	$5.000,00	D-S-SW
8	SG-008	Aplicar perfiles de seguridad	$0,00	D-S-SW-P
9	SG-009	Rediseño de red	$2.000,00	D-S-SW-HW-COM-MEDIA-AUX-L
10	SG-010	Herramienta de análisis de vulnerabilidad	$0,00	D-S-SW-HW-COM-MEDIA
11	SG-011	Limitar servicios y puertos vulnerables	$0,00	D-S-SW-HW-COM-MEDIA
12	SG-012	Actualización y mantenimiento	$0,00	D-S-SW-HW-COM-MEDIA
13	SG-013	Herramienta de monitorización de red	$0,00	D-S-SW-HW-COM-MEDIA
14	SG-014	Herramienta de análisis de software seguro	$0,00	D-S-SW
15	SG-015	Herramienta o software RADIUS	$2.000,00	D-S-SW-HW-COM-MEDIA
16	SG-016	UPS central para el centro de datos	$700,00	D-S-SW-HW-COM-MEDIA-AUX-L
17	SG-017	Seguridad Wireless	$0,00	D-S-SW-HW-COM-MEDIA

18	SG-018	Segmentación de la red	$0,00	D-S-SW-HW-COM-MEDIA
19	SG-019	Adquisición de firewall Fortigate	$2.000,00	D-S-SW-HW-COM-MEDIA
20	SG-020	Adquisición de servidor Dell	$9.000,00	D-S-SW-HW-COM-MEDIA
21	SG-021	Adquisición de 4 discos de 8 TB para QNAP	$1.400,00	D-S-SW-HW-COM-MEDIA
22	SG-022	Mantenimiento periódico al sistema de enfriamiento	$200,00	D-S-SW-HW-COM-MEDIA
23	SG-023	Control de acceso físico	$300,00	D-S-SW-HW-COM-MEDIA-AUX-L-P
24	SG-024	Formación y concientización	$2.000,00	D-S-SW-HW-COM-MEDIA-AUX-L-P
25	SG-025	Elaboración y ejecución de plan de recuperación de desastres	$0,00	D-S-SW-HW-COM-MEDIA-AUX-L-P
26	SG-026	Análisis y monitoreo de análisis de riesgo e impacto	$0,00	D-S-SW-HW-COM-MEDIA-AUX-L-P
27	SG-027	Elaboración y ejecución de plan de continuidad del negocio	$0,00	D-S-SW-HW-COM-MEDIA-AUX-L-P
28	SG-028	Verificar contratos con proveedores de servicios	$0,00	D-S-SW-HW-COM-MEDIA-AUX-L-P
29	SG-029	Solicitar información y estadísticas a proveedores	$0,00	D-S-SW-HW-COM-MEDIA-AUX-L-P
			$46.800,00	

8.6 Resumen riesgo final

Se realiza el cálculo del riesgo intrínseco, riesgo efectivo que brinda el riesgo que tenemos después de aplicar salvaguardas y el riesgo controlado por amenaza

Tabla 17 Detalle del resumen de riesgo intrínseco, efectivo y variación del riesgo por amenaza

Resumen Riesgo Intrínseco, Efectivo y variación del riesgo por amenaza					
			Riesgo diario por amenaza	Riesgo anual por amenaza	
N.º	Cod.	AMENAZA			

1	AM-01	Incendio	$537,02	$114.855,15	RIESGO INTRÍNSECO POR AMENAZA
			$53,70	$11.485,52	RIESGO EFECTIVO POR AMENAZA
			$483,32	$103.369,64	RIESGO CONTROLADO POR AMENAZA
2	AM-02	Desastre natural	$537,02	$114.855,15	RIESGO INTRÍNSECO POR AMENAZA
			$53,70	$11.485,52	RIESGO EFECTIVO POR AMENAZA
			$483,32	$103.369,64	RIESGO CONTROLADO POR AMENAZA
3	AM-03	Fallo / avería de Hardware (físico)	$107,15	$22.916,71	RIESGO INTRÍNSECO POR AMENAZA
			$10,72	$2.291,67	RIESGO EFECTIVO POR AMENAZA
			$96,44	$20.625,04	RIESGO CONTROLADO POR AMENAZA
4	AM-04	Fallo de servicios de comunicaciones	$224,25	$47.961,47	RIESGO INTRÍNSECO POR AMENAZA
			$22,43	$4.796,15	RIESGO EFECTIVO POR AMENAZA
			$201,83	$43.165,32	RIESGO CONTROLADO POR AMENAZA
5	AM-05	Avería climatización	$1.278,00	$273.332,25	RIESGO INTRÍNSECO POR AMENAZA
			$127,80	$27.333,23	RIESGO EFECTIVO POR AMENAZA
			$1.150,20	$245.999,03	RIESGO CONTROLADO POR AMENAZA
6	AM-06	Perdida de suministro de energía	$6.119,82	$1.308.876,50	RIESGO INTRÍNSECO POR AMENAZA
			$611,98	$130.887,65	RIESGO EFECTIVO POR AMENAZA
			$5.507,84	$1.177.988,85	RIESGO CONTROLADO POR AMENAZA
7	AM-07	Robo personal interno	$465,17	$99.487,16	RIESGO INTRÍNSECO POR AMENAZA
			$46,52	$9.948,72	RIESGO EFECTIVO POR AMENAZA
			$418,65	$89.538,45	RIESGO CONTROLADO POR AMENAZA
8	AM-08	Robo personas externas	$12.802,46	$2.738.125,06	RIESGO INTRÍNSECO POR AMENAZA
			$1.280,25	$273.812,51	RIESGO EFECTIVO POR AMENAZA
			$11.522,21	$2.464.312,56	RIESGO CONTROLADO POR AMENAZA

9	AM-09	Ataque informático	$16.990,83	$3.633.913,77	RIESGO INTRÍNSECO POR AMENAZA
			$1.699,08	$363.391,38	RIESGO EFECTIVO POR AMENAZA
			$15.291,75	$3.270.522,39	RIESGO CONTROLADO POR AMENAZA
10	AM-10	Vulnerabilidad de programas	$12.400,29	$2.652.112,02	RIESGO INTRÍNSECO POR AMENAZA
			$1.240,03	$265.211,20	RIESGO EFECTIVO POR AMENAZA
			$11.160,26	$2.386.900,82	RIESGO CONTROLADO POR AMENAZA
11	AM-11	Indisponibilidad lógica	$12.975,39	$2.775.111,54	RIESGO INTRÍNSECO POR AMENAZA
			$1.297,54	$277.511,15	RIESGO EFECTIVO POR AMENAZA
			$11.677,85	$2.497.600,38	RIESGO CONTROLADO POR AMENAZA
12	AM-12	Indisponibilidad personal	$147,42	$31.529,45	RIESGO INTRÍNSECO POR AMENAZA
			$14,74	$3.152,95	RIESGO EFECTIVO POR AMENAZA
			$132,68	$28.376,51	RIESGO CONTROLADO POR AMENAZA
13	AM-13	Errores humanos	$599,54	$128.225,55	RIESGO INTRÍNSECO POR AMENAZA
			$59,95	$12.822,55	RIESGO EFECTIVO POR AMENAZA
			$539,58	$115.402,99	RIESGO CONTROLADO POR AMENAZA
14	AM-14	Errores de configuración	$590,54	$126.300,67	RIESGO INTRÍNSECO POR AMENAZA
			$59,95	$12.822,55	RIESGO EFECTIVO POR AMENAZA
			$530,58	$113.478,12	RIESGO CONTROLADO POR AMENAZA
15	AM-15	Caída del sistema por agotamiento de recursos	$7.449,30	$1.593.219,04	RIESGO INTRÍNSECO POR AMENAZA
			$744,93	$159.321,90	RIESGO EFECTIVO POR AMENAZA
			$6.704,37	$1.433.897,13	RIESGO CONTROLADO POR AMENAZA
16	AM-16	Fuga de información	$459,27	$98.226,37	RIESGO INTRÍNSECO POR AMENAZA
			$45,93	$9.822,64	RIESGO EFECTIVO POR AMENAZA
			$413,34	$88.403,73	RIESGO CONTROLADO POR AMENAZA

17	AM-17	Acceso no autorizado	$19.663,16	$4.205.457,28	RIESGO INTRÍNSECO POR AMENAZA
			$1.966,32	$420.545,73	RIESGO EFECTIVO POR AMENAZA
			$17.696,84	$3.784.911,55	RIESGO CONTROLADO POR AMENAZA
18	AM-18	Fallo en copias	$1.458,00	$311.829,75	RIESGO INTRÍNSECO POR AMENAZA
			$145,80	$31.182,98	RIESGO EFECTIVO POR AMENAZA
			$1.312,20	$280.646,78	RIESGO CONTROLADO POR AMENAZA
19	AM-19	Manipulación de equipos	$6.946,97	$1.485.782,14	RIESGO INTRÍNSECO POR AMENAZA
			$694,70	$148.578,21	RIESGO EFECTIVO POR AMENAZA
			$6.252,27	$1.337.203,93	RIESGO CONTROLADO POR AMENAZA
20	AM-20	Modificación de la información	$12.400,29	$2.652.112,02	RIESGO INTRÍNSECO POR AMENAZA
			$1.240,03	$265.211,20	RIESGO EFECTIVO POR AMENAZA
			$11.160,26	$2.386.900,82	RIESGO CONTROLADO POR AMENAZA
21	AM-21	Errores de mantenimiento físico / actualización de programas	$19.873,80	$4.250.508,98	RIESGO INTRÍNSECO POR AMENAZA
			$1.987,38	$425.050,90	RIESGO EFECTIVO POR AMENAZA
			$17.886,42	$3.825.458,08	RIESGO CONTROLADO POR AMENAZA
22	AM-22	Difusión de software dañino	$15.206,94	$3.252.384,29	RIESGO INTRÍNSECO POR AMENAZA
			$1.520,69	$325.238,43	RIESGO EFECTIVO POR AMENAZA
			$13.686,25	$2.927.145,86	RIESGO CONTROLADO POR AMENAZA
23	AM-23	Destrucción de información	$459,27	$98.226,37	RIESGO INTRÍNSECO POR AMENAZA
			$45,93	$9.822,64	RIESGO EFECTIVO POR AMENAZA
			$413,34	$88.403,73	RIESGO CONTROLADO POR AMENAZA
24	AM-24	Pérdida de información	$12.400,29	$2.652.112,02	RIESGO INTRÍNSECO POR AMENAZA
			$4.213,62	$901.187,98	RIESGO EFECTIVO POR AMENAZA
			$8.186,67	$1.750.924,05	RIESGO CONTROLADO POR AMENAZA

Tabla 18 Detalle del resumen de riesgo intrínseco, efectivo y variación del riesgo por activo

Resumen Riesgo Intrínseco, Efectivo y variación del riesgo por activo			
	AC-01	AC-02	AC-03
	Respaldo de información de usuarios	Respaldo de servidores virtuales	Base de datos del sistema Ensurance
Riesgo intrínseco diario por activo	$2.209,50	$11.250,00	$13.725,00
Riesgo intrínseco anual por activo	$472.556,81	$2.406.093,75	$2.935.434,38
Riesgo efectivo diario por activo	$220,95	$1.125,00	$1.372,50
Riesgo efectivo anual por activo	$47.255,68	$240.609,38	$293.543,44
Riesgo controlado diario por activo	$1.988,55	$10.125,00	$12.352,50
Riesgo controlado anual por activo	$425.301,13	$2.165.484,38	$2.641.890,94
	AC-04	AC-05	AC-06
	Base de datos del sistema Auto nomina	Base de datos del sistema Helpdesk	Base de datos del sistema de Riesgo
Riesgo intrínseco diario por activo	$2.745,00	$74,64	$747,00
Riesgo intrínseco anual por activo	$587.086,88	$15.963,63	$159.764,63
Riesgo efectivo diario por activo	$493,20	$14,03	$74,70
Riesgo efectivo anual por activo	$105.483,15	$2.999,60	$15.976,46
Riesgo controlado diario por activo	$2.251,80	$60,62	$672,30
Riesgo controlado anual por activo	$481.603,73	$12.964,03	$143.788,16
	AC-07	AC-08	AC-09
	Base de datos del sistema Surving	Datos de servidor compartido	servicio de correo electrónico
Riesgo intrínseco diario por activo	$746,40	$12.510,00	$14.940,00
Riesgo intrínseco anual por activo	$159.636,30	$2.675.576,25	$3.195.292,50
Riesgo efectivo diario por activo	$74,64	$1.251,00	$2.587,50
Riesgo efectivo anual por activo	$15.963,63	$267.557,63	$553.401,56
Riesgo controlado diario por activo	$671,76	$11.259,00	$12.352,50
Riesgo controlado anual por activo	$143.672,67	$2.408.018,63	$2.641.890,94
	AC-10	AC-11	AC-12
	almacenamiento de ficheros NetBak	servicio página web	VMware vSphere
Riesgo intrínseco diario por activo	$14.940,00	$2.544,00	$13.725,00
Riesgo intrínseco anual por activo	$3.195.292,50	$544.098,00	$2.935.434,38
Riesgo efectivo diario por activo	$2.587,50	$254,40	$1.372,50
Riesgo efectivo anual por activo	$553.401,56	$54.409,80	$293.543,44
Riesgo controlado diario por activo	$12.352,50	$2.289,60	$12.352,50
Riesgo controlado anual por activo	$2.641.890,94	$489.688,20	$2.641.890,94
	AC-13	AC-14	AC-15
	Servicio emarine		

		Servidor de correo electrónico	Servidor Ensurance
Riesgo intrínseco diario por activo	$763,20	$13.725,00	$1.635,30
Riesgo intrínseco anual por activo	$163.229,40	$2.935.434,38	$349.749,79
Riesgo efectivo diario por activo	$98,19	$1.737,00	$163,53
Riesgo efectivo anual por activo	$21.000,39	$371.500,88	$34.974,98
Riesgo controlado diario por activo	$665,01	$11.988,00	$1.471,77
Riesgo controlado anual por activo	$142.229,01	$2.563.933,50	$314.774,81
	AC-16	AC-17	AC-18
	Servidor de página web	Servidor de Riesgo	Servidor de encuesta Surving
Riesgo intrínseco diario por activo	$747,00	$747,00	$746,40
Riesgo intrínseco anual por activo	$159.764,63	$159.764,63	$159.636,30
Riesgo efectivo diario por activo	$74,70	$140,31	$140,25
Riesgo efectivo anual por activo	$15.976,46	$30.008,80	$29.995,97
Riesgo controlado diario por activo	$672,30	$606,69	$606,15
Riesgo controlado anual por activo	$143.788,16	$129.755,82	$129.640,33
	AC-19	AC-20	AC-21
	Servidor Auto Nomina	Servidor de Helpdesk	Servidor de Antivirus
Riesgo intrínseco diario por activo	$750,60	$746,40	$670,80
Riesgo intrínseco anual por activo	$160.534,58	$159.636,30	$143.467,35
Riesgo efectivo diario por activo	$96,93	$96,51	$67,08
Riesgo efectivo anual por activo	$20.730,90	$20.641,08	$14.346,74
Riesgo controlado diario por activo	$653,67	$649,89	$603,72
Riesgo controlado anual por activo	$139.803,67	$138.995,22	$129.120,62
	AC-22	AC-23	AC-24
	Gestor de VM VMware vSphere	Veem Backup	Switch capa 2 TRENDnet
Riesgo intrínseco diario por activo	$9.990,00	$9.990,00	$417,60
Riesgo intrínseco anual por activo	$2.136.611,25	$2.136.611,25	$89.314,20
Riesgo efectivo diario por activo	$999,00	$999,00	$41,76
Riesgo efectivo anual por activo	$213.661,13	$213.661,13	$8.931,42
Riesgo controlado diario por activo	$8.991,00	$8.991,00	$375,84
Riesgo controlado anual por activo	$1.922.950,13	$1.922.950,13	$80.382,78
	AC-25	AC-26	AC-27
	Switch capa 2 D-Link	Switch capa 2 D-Link	CERAGON Radio Enlace
Riesgo intrínseco diario por activo	$417,60	$417,60	$39,33
Riesgo intrínseco anual por activo	$89.314,20	$89.314,20	$8.411,70
Riesgo efectivo diario por activo	$41,76	$41,76	$3,93
Riesgo efectivo anual por activo	$8.931,42	$8.931,42	$841,17
Riesgo controlado diario por activo	$375,84	$375,84	$35,40
Riesgo controlado anual por activo	$80.382,78	$80.382,78	$7.570,53
	AC-28	AC-29	AC-30
	Switch ADVA FSP 150-GE114Pro	Switch ADVA FSP 150-GE114Pro	Router Cisco C1111-8P

Riesgo intrínseco diario por activo	$452,70	$39,33	$452,70
Riesgo intrínseco anual por activo	$96.821,21	$8.411,70	$96.821,21
Riesgo efectivo diario por activo	$45,27	$3,93	$45,27
Riesgo efectivo anual por activo	$9.682,12	$841,17	$9.682,12
Riesgo controlado diario por activo	$407,43	$35,40	$407,43
Riesgo controlado anual por activo	$87.139,09	$7.570,53	$87.139,09
	AC-31	AC-32	AC-33
	Router Cisco C1111-8P	Cortafuegos Fortinet FortiGate 60D	Switch UniFi USW-Lite-16-PoE
Riesgo intrínseco diario por activo	$39,33	$1.513,00	$54,27
Riesgo intrínseco anual por activo	$8.411,70	$323.592,88	$11.607,00
Riesgo efectivo diario por activo	$3,93	$151,30	$5,43
Riesgo efectivo anual por activo	$841,17	$32.359,29	$1.160,70
Riesgo controlado diario por activo	$35,40	$1.361,70	$48,84
Riesgo controlado anual por activo	$7.570,53	$291.233,59	$10.446,30
	AC-34	AC-35	AC-36
	Consola UniFi UCK-G2-PLUS	Router Tp-Link Archer C80	Router Tp-Link
Riesgo intrínseco diario por activo	$39,33	$39,33	$39,33
Riesgo intrínseco anual por activo	$8.411,70	$8.411,70	$8.411,70
Riesgo efectivo diario por activo	$3,93	$3,93	$3,93
Riesgo efectivo anual por activo	$841,17	$841,17	$841,17
Riesgo controlado diario por activo	$35,40	$35,40	$35,40
Riesgo controlado anual por activo	$7.570,53	$7.570,53	$7.570,53
	AC-37	AC-38	AC-39
	Switch MikroTik RB2011iL-IN	Router Calix GigaHub	Switching Power Supply Mean Well
Riesgo intrínseco diario por activo	$6,56	$6,56	$4,08
Riesgo intrínseco anual por activo	$1.401,95	$1.401,95	$872,61
Riesgo efectivo diario por activo	$0,66	$0,66	$0,41
Riesgo efectivo anual por activo	$140,20	$140,20	$87,26
Riesgo controlado diario por activo	$5,90	$5,90	$3,67
Riesgo controlado anual por activo	$1.261,76	$1.261,76	$785,35
	AC-40	AC-41	AC-42
	Switch capa 3 DELL N1524	Switch capa 3 DELL N1524	HP ProLiant DL160 G6
Riesgo intrínseco diario por activo	$454,20	$39,33	$1.757,00
Riesgo intrínseco anual por activo	$97.142,03	$8.411,70	$375.778,38
Riesgo efectivo diario por activo	$45,42	$3,93	$175,70
Riesgo efectivo anual por activo	$9.714,20	$841,17	$37.577,84
Riesgo controlado diario por activo	$408,78	$35,40	$1.581,30
Riesgo controlado anual por activo	$87.427,82	$7.570,53	$338.200,54
	AC-43	AC-44	AC-45
	DELL PowerEdge R640	DELL PowerEdge R640	QNAP TS-1232XU-R

Riesgo intrínseco diario por activo	$2.007,00	$1.998,00	$1.998,00
Riesgo intrínseco anual por activo	$429.247,13	$427.322,25	$427.322,25
Riesgo efectivo diario por activo	$200,70	$199,80	$200,70
Riesgo efectivo anual por activo	$42.924,71	$42.732,23	$42.924,71
Riesgo controlado diario por activo	$1.806,30	$1.798,20	$1.797,30
Riesgo controlado anual por activo	$386.322,41	$384.590,03	$384.397,54
	AC-46	AC-47	AC-48
	DELL ME 4012	CLON Gigabyte H81M-H	Red Principal de Internet Level3
Riesgo intrínseco diario por activo	$2.007,00	$2.007,00	$586,05
Riesgo intrínseco anual por activo	$429.247,13	$429.247,13	$125.341,44
Riesgo efectivo diario por activo	$200,70	$200,70	$58,61
Riesgo efectivo anual por activo	$42.924,71	$42.924,71	$12.534,14
Riesgo controlado diario por activo	$1.806,30	$1.806,30	$527,45
Riesgo controlado anual por activo	$386.322,41	$386.322,41	$112.807,30
	AC-49	AC-50	AC-51
	Red de comunicaciones radio enlace	Red Secundaria de Internet Punto Net	Red inalámbrica
Riesgo intrínseco diario por activo	$428,40	$358,20	$546,00
Riesgo intrínseco anual por activo	$91.624,05	$76.610,03	$116.775,75
Riesgo efectivo diario por activo	$42,84	$35,82	$54,60
Riesgo efectivo anual por activo	$9.162,41	$7.661,00	$11.677,58
Riesgo controlado diario por activo	$385,56	$322,38	$491,40
Riesgo controlado anual por activo	$82.461,65	$68.949,02	$105.098,18
	AC-52	AC-53	AC-54
	Almacenamiento en red (SAN)	Discos virtuales (vdisk)	Cableado de datos
Riesgo intrínseco diario por activo	$1.323,00	$307,80	$783,00
Riesgo intrínseco anual por activo	$282.956,63	$65.830,73	$167.464,13
Riesgo efectivo diario por activo	$132,30	$30,78	$78,30
Riesgo efectivo anual por activo	$28.295,66	$6.583,07	$16.746,41
Riesgo controlado diario por activo	$1.190,70	$277,02	$704,70
Riesgo controlado anual por activo	$254.660,96	$59.247,65	$150.717,71
	AC-55	AC-56	AC-57
	Cableado eléctrico	Fibra óptica	Aire acondicionado York 18000 BTU
Riesgo intrínseco diario por activo	$234,90	$234,90	$199,35
Riesgo intrínseco anual por activo	$50.239,24	$50.239,24	$42.635,98
Riesgo efectivo diario por activo	$23,49	$23,49	$19,94
Riesgo efectivo anual por activo	$5.023,92	$5.023,92	$4.263,60
Riesgo controlado diario por activo	$211,41	$211,41	$179,42
Riesgo controlado anual por activo	$45.215,31	$45.215,31	$38.372,38
	AC-58	AC-59	AC-60

	Aire acondicionado centralizado	Sistema de alimentación ininterrumpida E-T-N POWERWARE	Rack de comunicaciones
Riesgo intrínseco diario por activo	$278,10	$230,25	$7,20
Riesgo intrínseco anual por activo	$59.478,64	$49.244,72	$1.539,90
Riesgo efectivo diario por activo	$27,81	$23,03	$0,72
Riesgo efectivo anual por activo	$5.947,86	$4.924,47	$153,99
Riesgo controlado diario por activo	$250,29	$207,23	$6,48
Riesgo controlado anual por activo	$53.530,77	$44.320,25	$1.385,91
	AC-61	AC-62	AC-63
	Rack de servidores	Cuarto del centro de procesamiento de datos	Jefe de Sistemas
Riesgo intrínseco diario por activo	$7,20	$7.710,75	$966,60
Riesgo intrínseco anual por activo	$1.539,90	$1.649.136,66	$206.731,58
Riesgo efectivo diario por activo	$0,72	$771,08	$96,66
Riesgo efectivo anual por activo	$153,99	$164.913,67	$20.673,16
Riesgo controlado diario por activo	$6,48	$6.939,68	$869,94
Riesgo controlado anual por activo	$1.385,91	$1.484.222,99	$186.058,42
	AC-64	AC-65	
	Administrador de redes y base de datos	Asistente de Helpdesk	
Riesgo intrínseco diario por activo	$9,45	$966,60	
Riesgo intrínseco anual por activo	$2.021,12	$206.731,58	
Riesgo efectivo diario por activo	$0,95	$96,66	
Riesgo efectivo anual por activo	$202,11	$20.673,16	
Riesgo controlado diario por activo	$8,51	$869,94	
Riesgo controlado anual por activo	$1.819,01	$186.058,42	

8.7 Resultado diario por activo

Tenemos una comparación del riesgo intrínseco o riesgo actual, riesgo efectivo después de aplicar salvaguardas y el resultado final que es el riesgo controlado por cada activo después de la aplicación de las recomendaciones.

Tabla 18 Detalle del resultado diario por activo

N.º	Código	Nombre	Riesgo intrínseco total diario	Riesgo efectivo total diario	Riesgo controlado por salvaguardas
1	D-1	Respaldo de información de usuarios	$2.209,50	$220,95	$1.988,55

2	D-2	Respaldo de servidores virtuales	$11.250,00	$1.125,00	$10.125,00
3	D-3	Base de datos del sistema Ensurance	$13.725,00	$1.372,50	$12.352,50
4	D-4	Base de datos del sistema Auto nomina	$2.745,00	$493,20	$2.251,80
5	D-5	Base de datos del sistema Helpdesk	$74,64	$14,03	$60,62
6	D-6	Base de datos del sistema de Riesgo	$747,00	$74,70	$672,30
7	D-7	Base de datos del sistema Surving	$746,40	$74,64	$671,76
8	D-8	Datos de servidor compartido	$12.510,00	$1.251,00	$11.259,00
9	S-1	servicio de correo electrónico	$14.940,00	$2.587,50	$12.352,50
10	S-2	almacenamiento de ficheros NetBak	$14.940,00	$2.587,50	$12.352,50
11	S-3	servicio página web	$2.544,00	$254,40	$2.289,60
12	S-4	VMware vSphere	$13.725,00	$1.372,50	$12.352,50
13	S-5	Servicio emarine	$763,20	$98,19	$665,01
14	SW-1	Servidor de correo electrónico	$13.725,00	$1.737,00	$11.988,00
15	SW-2	Servidor Ensurance	$1.635,30	$163,53	$1.471,77
16	SW-3	Servidor de página web	$747,00	$74,70	$672,30
17	SW-4	Servidor de Riesgo	$747,00	$140,31	$606,69
18	SW-5	Servidor de encuesta Surving	$746,40	$140,25	$606,15
19	SW-6	Servidor Auto Nomina	$750,60	$96,93	$653,67
20	SW-7	Servidor de Helpdesk	$746,40	$96,51	$649,89
21	SW-8	Servidor de Antivirus	$670,80	$67,08	$603,72
22	SW-9	Gestor de VM VMware vSphere	$9.990,00	$999,00	$8.991,00
23	SW-10	Veem Backup	$9.990,00	$999,00	$8.991,00
24	HW-1	Switch capa 2 TRENDnet	$417,60	$41,76	$375,84
25	HW-2	Switch capa 2 D-Link	$417,60	$41,76	$375,84
26	HW-3	Switch capa 2 D-Link	$417,60	$41,76	$375,84
27	HW-4	CERAGON Radio Enlace	$39,33	$3,93	$35,40
28	HW-5	Switch ADVA FSP 150-GE114Pro	$452,70	$45,27	$407,43
29	HW-6	Switch ADVA FSP 150-GE114Pro	$39,33	$3,93	$35,40
30	HW-7	Router Cisco C1111-8P	$452,70	$45,27	$407,43
31	HW-8	Router Cisco C1111-8P	$39,33	$3,93	$35,40
32	HW-9	Cortafuegos Fortinet FortiGate 60D	$1.513,00	$151,30	$1.361,70

33	HW-10	Switch UniFi USW-Lite-16-PoE	$54,27	$5,43	$48,84
34	HW-11	Consola UniFi UCK-G2-PLUS	$39,33	$3,93	$35,40
35	HW-12	Router Tp-Link Archer C80	$39,33	$3,93	$35,40
36	HW-13	Router Tp-Link	$39,33	$3,93	$35,40
37	HW-14	Switch MikroTik RB2011iL-IN	$6,56	$0,66	$5,90
38	HW-15	Router Calix GigaHub	$6,56	$0,66	$5,90
39	HW-16	Switching Power Supply Mean Well	$4,08	$0,41	$3,67
40	HW-17	Switch capa 3 DELL N1524	$454,20	$45,42	$408,78
41	HW-18	Switch capa 3 DELL N1524	$39,33	$3,93	$35,40
42	HW-19	HP ProLiant DL160 G6	$1.757,00	$175,70	$1.581,30
43	HW-20	DELL PowerEdge R640	$2.007,00	$200,70	$1.806,30
44	HW-21	DELL PowerEdge R640	$1.998,00	$199,80	$1.798,20
45	HW-22	QNAP TS-1232XU-R	$1.998,00	$200,70	$1.797,30
46	HW-23	DELL ME 4012	$2.007,00	$200,70	$1.806,30
47	HW-24	CLON Gigabyte H81M-H	$2.007,00	$200,70	$1.806,30
48	COM-1	Red Principal de Internet Level3	$586,05	$58,61	$527,45
49	COM-2	Red de comunicaciones radio enlace	$428,40	$42,84	$385,56
50	COM-3	Red Secundaria de Internet Punto Net	$358,20	$35,82	$322,38
51	COM-4	Red inalámbrica	$546,00	$54,60	$491,40
52	MEDIA-1	Almacenamiento en red (SAN)	$1.323,00	$132,30	$1.190,70
53	MEDIA-2	Discos virtuales (vdisk)	$307,80	$30,78	$277,02
54	AUX-1	Cableado de datos	$783,00	$78,30	$704,70
55	AUX-2	Cableado eléctrico	$234,90	$23,49	$211,41
56	AUX-3	Fibra óptica	$234,90	$23,49	$211,41
57	AUX-4	Aire acondicionado York 18000 BTU	$199,35	$19,94	$179,42
58	AUX-5	Aire acondicionado centralizado	$278,10	$27,81	$250,29
59	AUX-6	Sistema de alimentación ininterrumpida E-T-N POWERWARE	$230,25	$23,03	$207,23
60	AUX-7	Rack de comunicaciones	$7,20	$0,72	$6,48
61	AUX-8	Rack de servidores	$7,20	$0,72	$6,48
62	L-1	Cuarto del centro de procesamiento de datos	$7.710,75	$771,08	$6.939,68
63	P-1	Jefe de Sistemas	$966,60	$96,66	$869,94

64	P-2	Administrador de redes y base de datos	$9,45	$0,95	$8,51
65	P-3	Asistente de Helpdesk	$966,60	$96,66	$869,94

9. Propuestas para continuidad del negocio

Detallamos varias propuestas significativas que ayudarán a tener una mejor respuesta en el caso de que se presente algún incidente.

9.1 Rediseño de la red

En esta etapa vamos a proceder a proponer un rediseño de la red a corto y largo plazo para así superar las debilidades del diseño actual y mejorar la seguridad de la información.

9.1.1 Debilidades del diseño actual

La topología de la red actualmente tiene las siguientes debilidades:

- No existe una segmentación adecuada por cuanto los computadores de los usuarios y servidores del centro de datos se encuentran conectados a una sola subred.
    - Debido a lo anterior, existe el riesgo de que, si el dispositivo de un empleado se infectase con malware, éste se propague a otras estaciones o servidores convirtiéndose en una amenaza de seguridad de la información de la compañía.
- Existen servidores con sistemas operativos Windows 2003-2008 Server, estaciones con Windows 7, los cuales ya no están bajo soporte de Microsoft.
    - Esto hace posible que, si un atacante tuviese acceso a la red local, podría aprovechar vulnerabilidades conocidas para las que Microsoft ya no provee parches y acceder al control de los equipos.

- El diseño actual de red no cumple con criterios de arquitectura de seguridad y defensa en profundidad.

9.1.2 Diseño de red propuesto

Con el fin de proteger adecuadamente la data de la compañía se procederá a definir un diseño de red seguro.

La norma ISO 27001, nos ofrece varias recomendaciones sobre buenas prácticas para la gestión de seguridad de la información. Donde debemos tener en cuenta 3 factores fundamentales como lo son:

- Confidencialidad: Donde aseguramos que la información sea accesible solo a personas autorizadas.
- Integridad: Asegurar que la información sea exacta y completa en su totalidad.
- Disponibilidad: Asegurar que los usuarios autorizados tengan acceso a la información cuando lo requieran.

Para tener una adecuada seguridad lógica definiremos una configuración en base a los criterios descritos anteriormente, en donde evitemos el acceso no autorizado a los recursos ya sea vía local o vía red.

Con base a la situación actual y el objetivo de negocio de la compañía se plantea el siguiente rediseño de red a corto plazo el cual es escalable y constituye un paso intermedio hasta llegar a la red ideal.

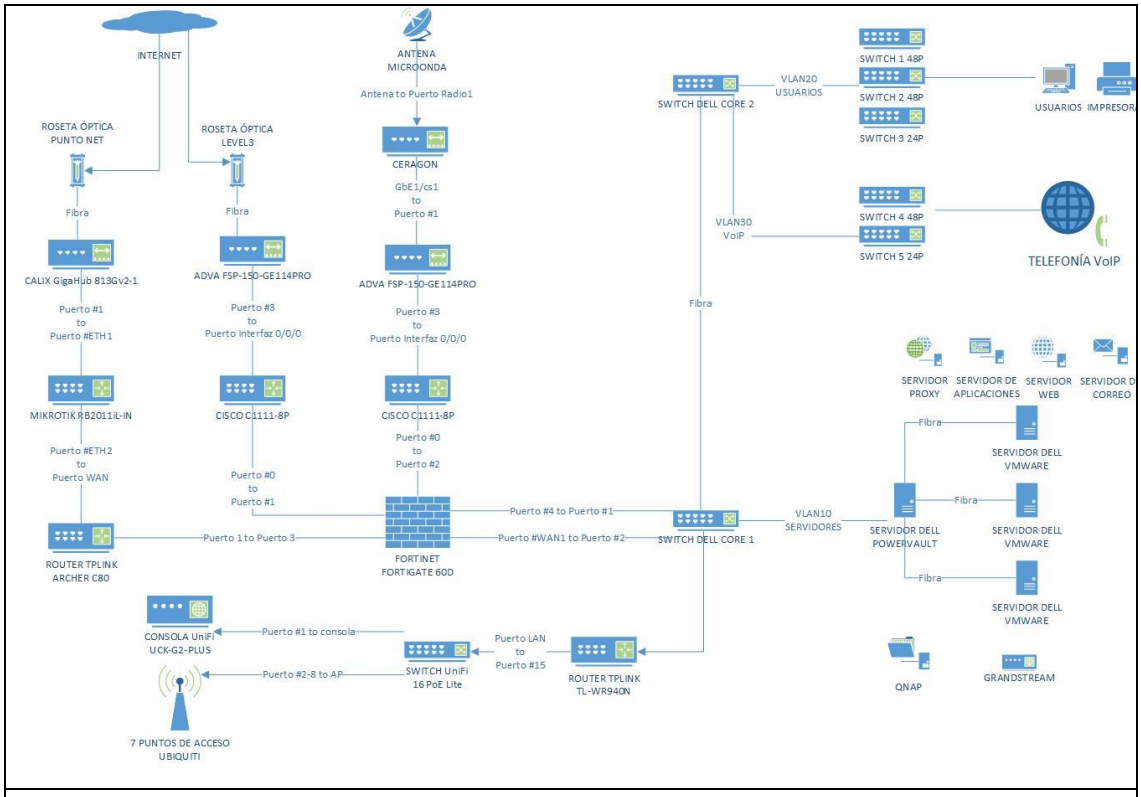


Figura 17: Topología de red a corto plazo
Fuente: Autor

Y a su vez proponemos un rediseño de red a largo plazo, el cual incorpora criterios de arquitectura de seguridad y defensa en profundidad.

Cabe indicar que el diseño de red que se plantea cumple con el tercer objetivo de la seguridad de la información, esto es disponibilidad, debido a que el diseño es modular, escalable e incluye redundancia en los elementos críticos como switch Core, firewalls de borde y conexiones de respaldo hacia los mismos, sin embargo para que en la práctica se almacenen tanto disponibilidad, como la confidencialidad e integridad, es necesario que los equipos y servidores cuenten con elementos de hardware redundantes y que se realicen recomendaciones a nivel software y protocolos que permitan cumplir con estos objetivos.

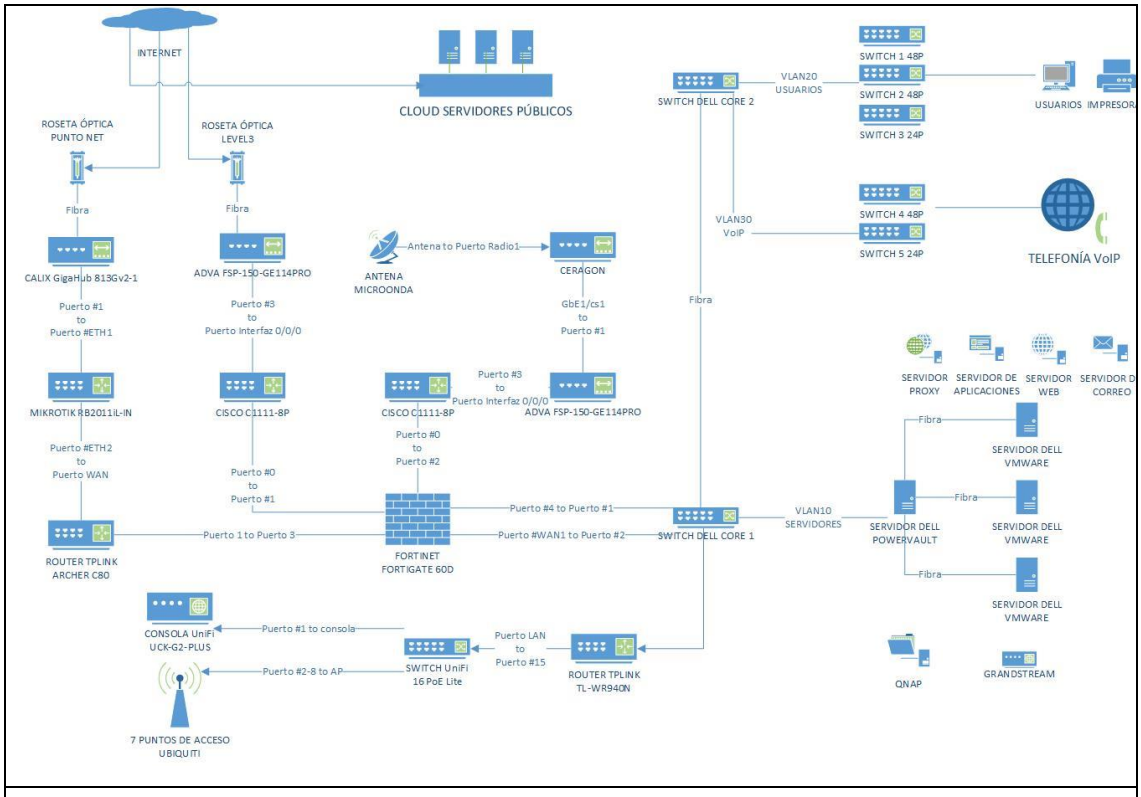


Figura 17: Topología de red a largo plazo
Fuente: Autor

9.1.3 Implementación y cumplimiento de políticas de seguridad

Se debe definir una Política de Seguridad Informática que esté enmarcada bajo el estándar internacional ISO 27001 y que incluya como mínimo los puntos detallados a continuación:

- Seguridad ambiental y física
- Identificación de procedimientos operacionales
- Políticas de control de acceso
    - Responsabilidades de usuarios
    - Control de acceso a la red
    - Control de acceso a sistemas operativos
    - Control de acceso a las aplicaciones e información
    - Comunicaciones móviles, correo electrónico e internet.
- Políticas de respaldo y restauración

- Procedimientos de monitoreo y manejo de incidentes
- Políticas de contingencia y continuidad del negocio

Se plantea también incorporar la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) que nos permita efectuar todos los procesos de forma segura.

Se recomienda que el centro de datos cumpla con estándares como EPA TIER 3.

Para que la compañía mantenga un diseño seguro actualizado se recomienda efectuar una Auditoria de Seguridad Informática anual tanto interna como externa.

9.1.4 Prácticas de seguridad de red recomendadas

Presentamos algunas de las amenazas más comunes en los entornos empresariales:

- Abuso de la red: Donde se presentan uso de aplicaciones no aprobadas por parte de los empleados o personas externas, acceso a contenidos no relacionados con la operación de la compañía.
- Disrupción de servicios: disrupciones en las aplicaciones, infraestructura y otros recursos del negocio ocasionados por virus, botnet, gusanos, malware, adware, spyware, ransomware, ataques de denegación de servicios (DoS) y ataques de capa 2.
- Accesos no autorizados: escalación de privilegios, intrusiones, accesos no autorizados a recursos restringidos.
- Robo de identidad y fraude: robo de datos personales o fraude en servidores y estaciones de usuarios a través de phishing o spam.
- Perdida de datos: perdida o filtración de información privada desde servidores o puntos finales mientras la información esté en tránsito o como resultado de un malware, virus, uso de keyloggers, etc.

Para evitar dichas amenazas el rediseño de red se complementará con un diseño de seguridad lógica enfocado en los elementos claves que definimos a continuación:

- Protección fundamental de red
- Hardening de dispositivos y servidores a través de la infraestructura de red
- Asegurar la disponibilidad, resistencia e integridad de la infraestructura de red
- Protección a nivel perimetral
    - Conexión segura hacia internet
    - Protección de los recursos internos y usuarios de software malicioso
    - Proteger a los usuarios de contenido dañino
    - Forzando la aplicación de políticas de correo electrónico navegación para prevenir robo de identidad y fraude.
    - Bloqueando comandos y controlando el tráfico de bots internos hacia host externos.
- Protección del centro de datos
    - Se asegura la disponibilidad e integridad de los sistemas y aplicaciones centralizadas
    - Protegiendo la confidencialidad y privacidad de datos sensibles.
- Seguridad y control de acceso a la red
    - Asegurando los perímetros de acceso
    - Requiriendo la autenticación y acceso basado en roles
    - Activando el doble factor de autenticación en los servidores y aplicativos críticos.
- Movilidad segura
- Proveyendo seguridad, protección contra virus y conectividad persistente, requiriendo encriptación, autenticación y acceso basado en roles a todos los usuarios móviles.
- Asegurando que todos los sistemas cumplan con políticas corporativas y estén actualizados en materia de seguridad.

Estas áreas de seguridad claves en conjunto proveerán una solución de defensa integral para proteger al centro de datos de la compañía contra amenazas comunes de seguridad.

9.1.5 Protección fundamental de red

Nuestro diseño de red incluye routers, switches, firewall y otros dispositivos de infraestructura de red que mantienen ejecutándose servicios y aplicaciones. Estos dispositivos deben garantizar la operación continua y mantener el acceso a los mismos.

Para asegurar la disponibilidad de la infraestructura de red se recomienda las siguientes prácticas de seguridad:

- Acceso a dispositivos de infraestructura
    - Restringir el acceso administrativo a los dispositivos, solo el personal autorizado.
    - Exigir autenticación, autorización y llevar un registro de actividades a través del protocolo Remote Authentication Dial-In User Service (RADIUS) para autenticar el acceso, autorizar acciones y registrar todos los accesos administrativos.
    - Implementar la verificación de dos pasos o doble factor de autenticación, para garantizar la identidad del usuario.
    - Mostrar anuncios informativos que detallen el acceso exclusivo del personal autorizado
    - Asegurar la confidencialidad a través de protocolos seguros como Secure Shell (SSH), HTTPS, SNMPv3
    - Configurar tiempo de expiración de sesión desatendida.
- Infraestructura de routers
    - Solicitando a nuestro ISP el filtrado de rutas para asegurar que sólo se adviertan redes legitimas y que nunca se propaguen las redes que se supone no deben ser compartidas
    - Solicitando al ISP activar el registro de eventos significativos.
- Resistencia de dispositivos y supervivencia
    - Realizando Hardening de servicios, es decir deshabilitar todos aquellos servicios, aplicaciones, módulos de kernel que no sean necesarios para el funcionamiento adecuado del dispositivo.

- Mantenimiento de las contraseñas y control de acceso a los equipos.
- Implementando políticas a nivel de panel de control
- Habilitando control de tormentas de tráfico
- Habilitando trazabilidad sobre cada servidor o aplicaciones
- Implementando redundancia a nivel de topología, sistemas y módulos para proveer alta disponibilidad y supervivencia de ruteadores, switches y firewall
- Mantener estadísticas locales en los dispositivos

- Telemetría de red
  - Habilitar sincronización de tiempo a través del protocolo Network Time Protocol (NTP)
  - Recolectar información de estado y eventos de los sistemas a través de Syslog, RADIUS.
  - Monitorear el uso de CPU, memoria, accesos fallidos o no y tareas ejecutadas en sistemas críticos
  - Habilitar herramientas para monitoreo de tráfico y seguridad de red
  - Recolectar información para su posterior análisis
- Exigir cumplimiento de políticas de red
  - Implementar filtros de acceso (ACLs) en el perímetro de la red y en el aplicativo firewall-host de cada servidor
  - Configurar protección contra suplantación de IPs con ACLs y Unicast Reverse Path Forwarding (URPF) en routers o firewall de borde.
- Infraestructura conmutada
  - Implementar el diseño jerárquico de red a nivel lógico a través de la segmentación de la LAN en diferentes subredes IPs con redes virtuales VLANs para reducir el tamaño de los dominios de broadcast
  - La configuración más usual consiste en agrupar a los usuarios/dispositivos en redes virtuales por departamento. Ejemplo vlan de gerencia, vlan de servidores internos, etc.
  - Para que esto sea posible los dispositivos de comunicaciones deben soportar el protocolo IEEE 802.1q

- Se recomienda crear como mínimo las siguientes redes virtuales a corto plazo.
    - Vlan Nativa: Se debe reemplazar la vlan 1 por defecto por un identificador diferente en todos los switches.
    - Vlan servidores internos: que incluyan todos los servidores
    - Vlan de Voz: que incluya la central de voz/ip
    - Vlan Usuarios: que incluyan todos los usuarios de la compañía.
- A largo plazo se recomienda también crear las siguientes redes virtuales adicionales:
    - Vlan servidores locales: que incluyan los servidores de respaldos, monitoreo, logs, etc. Separándolos de la vlan de servidores internos.
    - Vlan servidores Bases de datos: para poder separar los servidores de las bases de datos.
    - Vlan departamentales: una vlan por departamento
- A nivel de red perimetral debe existir también segmentación
    - Se deben configurar las VLANs separadas para las conexiones hacia internet
    - Se recomienda usar los servicios de un proveedor de nube para alojar los servidores públicos como el correo electrónico, página web, emarine.
- Se debe proteger el protocolo Spanning Tree Protocol STP de posibles ataques a la topología:
    - Los puertos que sirven como enlaces entre switches deben configurarse como puertos troncales (trunk)
    - Los puertos de los switches a los que van conectados dispositivos de usuario final como PC, servidores, impresoras deben configurarse en modo acceso fijo (Access)
    - Ningún puerto de ningún switch debe dejarse en modo automático (auto) para evitar ataques internos al protocolo 802.1q

- Los puertos de los firewalls internos y externos deberán configurarse en modo troncal (trunk) y tener tantas interfaces lógicas (subinterfaces) configuradas como a VLANs den acceso
- Si los switches lo permiten se debe usar de preferencia Per-VLAN Spanning Tree (PVST) para reducir el alcance de los posibles daños o ataques
- Los puertos libres de los switches que no se estén utilizando deben deshabilitarse (Down) y colocarse en una vlan que no se use
- Configurar protección de puertos y de los protocolos ARP y DHCP

- Red inalámbrica
  - Se debe adquirir un router que brinde servicio DHCP para la red Ubiquiti que tiene la compañía
  - Se debe configurar al menos una vlan para invitados con acceso solo a internet y aislada de la red corporativa.
  - El acceso a la vlan invitados debe manejarse a través de usuario y contraseña con tiempo de vida limitado
  - El acceso de los usuarios a la vlan corporativa deberá controlarse a través del protocolo IEEE 802.1X. Por este motivo deberá configurarse el protocolo RADIUS en el controlador inalámbrico para verificar la información de autenticación con el servidor ABC
- Administración de la red
  - Asegurar la administración segura de todos los dispositivos y hosts dentro de la infraestructura de red de la compañía
  - Autenticar, autorizar y mantener registros de todos los accesos administrativos
  - Se debe implementar una red separada de administración de la red, todos los equipos deben tener una ip asignada para la administración remota vía red mediante protocolos seguros ssh, https, snmpv3. La

consola de correlación de eventos también debe estar asignada a esta vlan.

- Control de puntos finales
    - Se debe mantener actualizada la base de datos del antivirus que posee la compañía.
    - Desde la consola del antivirus controlar los puertos periféricos, bloquear accesos a paginas restringidas, bloquear acceso a instalación de aplicaciones.
    - Configurar la consola para que emita alertas vía correo electrónico, y tener un constante monitoreo para una buena gestión.
- Control de acceso
    - A largo plazo se debe implementar mecanismos de identificación para controlar el acceso a la red (IBNS – Identity Based Network Services)
    - El objetivo de implementar IBNS es que el administrador de red pueda aplicar políticas de seguridad especificas por usuario, y así poder identificar y autorizar en base a la identidad.
    - Aquellos equipos que no cumplan con las políticas de seguridad, podrán ser colocados en una vlan de cuarentena aislada de las subredes internas de la compañía
    - Para cumplir con esta implementación los equipos tales como switches, puntos de acceso inalámbricos, routers, firewalls, servidores y estaciones de trabajo deberán soportar e implementar protocolo IEEE 802.1X
    - La autenticación de los clientes debe ser centralizada hacia un servidor ABC que implemente el protocolo RADIUS y la distribución de claves de cifrado debe ser dinámica, por este motivo todos los dispositivos autenticadores deberán soportar el protocolo RADIUS
    - El servidor ABC deberá proveer una base de datos local, y debe integrarse con base de datos externas vía ODBC, para la administración de perfiles de usuarios, grupos, equipos autenticadores y políticas de control de acceso

- Para la preadmisión se recomienda mínimo las siguientes políticas:
  - Verificación de credenciales del usuario
  - Sistema operativo del equipo debe tener aplicados los últimos parches de seguridad recomendados por el fabricante
  - Sistema operativo del equipo debe tener instalado un antivirus con la base de firmas actualizadas.
- El servidor ABC deberá guardar un registro (log) de los accesos fallidos, exitosos y de las acciones autorizadas y desautorizadas de los usuarios. El administrador de red deberá revisar periódicamente el registro de logs con el fin de detectar intentos de ingreso no autorizados.

9.1.6 Protección perimetral

Definimos con red perimetral a la parte de la infraestructura de red que provee conectividad hacia internet. El perímetro debe proveer acceso centralizado seguro hacia el internet y usuarios invitados de la compañía.

También debe proveer acceso desde internet hacia los servicios públicos como el servidor web, sin comprometer la confidencialidad integridad y disponibilidad de los recursos y datos de la compañía.

Para proveer acceso seguro, la red perimetral debe incorporar las funciones de seguridad detalladas a continuación:

- Ruteadores de borde: el ruteador es la primera línea de defensa en contra de amenazas externas y debe tener siempre su sistema operativo actualizado y parchado, sus servicios deben ser minimizados (Hardening) y deberá ser protegido en base a las recomendaciones dadas en el punto 2.17.5
- Firewall externo: el firewall debe ser de próxima generación NGFW, para así poder proteger los recursos de la compañía de accesos no autorizados, el firewall debe identificar aplicaciones y soportar filtros para detección y

bloqueo de tráfico del contenido de aplicaciones, botnet, malware o ataques polimórficos. Se deben configurar reglas de filtrado para evitar el ingreso a la red privada desde internet y deben incorporarse reglas para proteger servidores públicos en la dmz como el portal web, emarine, servidor de correo. Se debe controlar además el tráfico desde la red interna hacia el internet, para que los usuarios y aplicativos autorizados puedan salir. Si algunos usuarios necesitan conectarse desde fuera de la compañía se recomienda usar VPN red privada virtual para que lo realicen de forma segura. Y también adquirir un firewall para realizar una administración de seguridad propia en la compañía y no depender del firewall externo.

- Prevención de intrusos y de amenazas avanzadas: Tanto el firewall externo como el interno deben incluir un sistema de prevención de intrusos IPS para detección, mitigación de las amenazas, también un módulo para la detección y prevención de amenazas avanzadas y malware de día cero. El IPS será responsable por identificar y bloquear tráfico anómalo o paquetes reconocidos como tráfico malicioso o ataques bien conocidos. El IPS nos debe brindar la posibilidad al administrador de red de bloquear ciertas aplicaciones de internet.
- Zona desmilitarizada DMZ: el servidor de correo, portales web y otros servidores públicos deben ser colocados en la DMZ con propósitos de seguridad y control. La DMZ va a actuar como un estado intermedio entre los recursos de la red interna e internet, evitando que los usuarios externos accedan de firma directa a los servidores y datos internos de la compañía. Los firewalls de borde serán responsables de restringir el tráfico entrante hacia los servidores públicos en la DMZ y controlar los accesos salientes desde la DMZ hacia internet. Los sistemas que residan en la DMZ deben ser asegurados (Hardening) y contar con software para protección de puntos finales que incluya protección contra amenazas avanzadas. A largo plazo con el fin de ahorrar costos de ancho de banda y minimizar la exposición de la red local hacia internet, se sugiere migrar los servidores públicos hacia la nube.

- Seguridad de correo electrónico: Los firewalls de borde interno y externo deberán contar con mecanismos para protección de amenazas comunes al correo electrónico, previo a la entrega de correos al servidor o estaciones internas. Además, contamos con un sistema Anti-X (anti-phishing, anti-spam, anti-malware).
- Seguridad web: Los firewalls de borde interno y externo deberán contar con filtrado de URLs en base a categorías y reputación, adicionalmente deberán brindar protección contra ataques comunes como SQL injection, web Shell, etc.

9.1.7 Detalle de equipos a nivel de Seguridad Lógica

Detalle de equipos que se van a reutilizar y equipos que se sugieren adquirir para tener una distribución apropiada a nivel de seguridad lógica

Con relación a la Capa Core + Distribución detallamos

- Se conservan los servidores DELL EMC (VMware ESXI)
- Se recomienda la adquisición de un gestor de eventos de seguridad SIEM
    - El sistema de correlación de eventos puede ser un dispositivo de propósito especifico (APPLIANCE) o bien un aplicativo/software instalado sobre un equipo servidor
    - A corto plazo debe cumplir con las siguientes características:
        - Descubrimiento e inventario de activos
        - Analizador de vulnerabilidades
        - Detección de intrusiones
        - Monitoreo de comportamiento
        - Correlación de eventos
    - A largo plazo debemos implementar las siguientes características:
        - Administración de logs
        - Monitoreo de activos en nube
        - Monitoreo de aplicaciones en nube

- Automatización y orquestado de seguridad
- Integración con sistemas de tickets
- Inteligencia continua de amenazas
- Dashboard avanzado para la visualización de amenazas en tiempo real

- Se recomienda adquirir un switch capa 3 administrable
  - El switch debe tener fuente de poder redundante para tener disponibilidad en caso de que 1 fuente falle.
  - Debe tener como mínimo estos requisitos de seguridad:
    - Protección contra ataques de denegación de servicio, dirigidos hacia el procesador de rutas
    - Protección contra ataques de suplantación (spoofing) de direcciones Mac y direcciones ip
    - Administración mediante interfaz gráfica y/o línea de comandos a través de puerto de consola
    - Control del acceso administrativo al switch a través de cuentas de usuarios con contraseñas
    - Mecanismos de seguridad de puertos y control de acceso al medio
    - Mecanismo seguro para recuperar la contraseña del administrador si se pierde accidentalmente
    - El fabricante del equipo debe proveer regularmente actualizaciones de software y parches de seguridad
  - Adicionalmente el switch debe soportar los siguientes protocolos:
    - IEEE 802.3 ETHERNET
    - IEEE 802.3U FAST ETHERNET
    - IEEE 802.3Z 1000BASE-SX/LX
    - IEEE 802.3AB 1000BASE-T
    - IEEE 802.3AE 10 GIGABIT ETHERNET
    - IEEE 802.1D STP
    - IEEE 802.1Q VLAN
    - IEEE 802.1X AUTHENTICATION AND KEY MANAGEMENT

- IEEE 802.3X FULL-DUPLEX FLOW CONTROL
- RFC 768 UDP
- RFC791 IP
- RFC 792ICMP
- RFC 826 ARP
- RFC 2068 HTTP
- DHCP / BOOTP RELAY
- DNS
- NTP
- SNMPV3
- RFC 791 IP
- RFC 2460 IPv6 (pass-through Bridging mode)
- RFC 792 ICMP
- RFC 793 TCP
- RFC 826 ARP
- RFC 2131 DHCP
- RFC 2068 HTTP
- SNMPV3

- Se conservan puntos de acceso Ubiquiti

Con relación a la capa de acceso detallamos lo siguiente

- Se conserva los 2 switch capa 2 Dlink y 1 switch capa 2 TRENDnet
- Se conserva el controlador inalámbrico Ubiquiti
- Se recomienda adquirir un router DHCP robusto para la red inalámbrica.
- Se recomienda adquirir 4 switch capa 2 de 24 puertos para realizar una distribución más ordenada en la planta alta.
- Se recomienda adquirir 2 switch capa 2 de 24 puertos para redistribuir la red en la planta baja
- Se recomienda adquirir 3 puntos de acceso ubiquiti adicionales para una mayor cobertura en la empresa.

Con relación a las conexiones externas y de red desmilitarizadas

- Se conserva el router de borde y el firewall Fortigate 60E que son de propiedad de nuestro ISP
- Se recomienda adquirir un Firewall Fortigate 60E para que sea administrado exclusivamente por el administrador de red de la compañía y puedan crear las políticas necesarias sin depender de un proveedor.
- Usar 1 switch capa 3 de los que tiene la compañía exclusivamente para la DMZ y conexiones con proveedores

9.1.8 Nube de servidores públicos

El diseño de red a largo plazo sugiere migrar los servidores públicos ubicados en la DMZ hacia un proveedor en la nube

Para efectuar dicha migración la compañía debe plantear algunas interrogantes como lo son:

- ¿Cuál es el rol de la compañía en la protección de sus datos y cuál es el rol del proveedor en la mitigación de incidentes y protección de los datos
- ¿Cuáles transmisiones de datos especificas cifra el proveedor?
- ¿Dónde residen físicamente los servidores provistos a Seguros la Unión? Esta pregunta es fundamental debido a la legislación de protección de datos personales.
- ¿Quién tiene acceso a los datos de Seguros la Unión en la nube?
- ¿Cuál es la política del proveedor para que nos asegure que solo empleados autorizados van a poder acceder a los datos de la compañía?
- ¿Cuál es el tiempo de operación (uptime) que garantizan en el contrato de servicios (SLA)?
- ¿Cuál es el proceso a seguir cuando se sospecha de una violación de seguridad?

- ¿Efectúa el proveedor pruebas de intrusión sobre los sistemas provistos a la compañía? Si la respuesta es sí ¿Podemos tener acceso a los informes de resultados?
- ¿Cuál es el procedimiento a seguir para que la compañía realice de manera propia pruebas de intrusión sobre sus sistemas alojados en nube?
- ¿Cómo protege el proveedor el acceso a GUIs y APIs?
- ¿Cuáles son los términos del proveedor respecto a la propiedad de los datos?
- ¿Cuáles son las medidas de seguridad que dispone el proveedor para proteger sus centros de datos?
- ¿Cuál es el nivel de soporte incluido en el SLA estándar?
- ¿Se incluye la realización de respaldos en el SLA estándar?
- ¿Qué tipo de respaldos realiza el proveedor y con qué frecuencia?
- ¿Tiene el proveedor un plan de recuperación ante desastres? ¿Con que frecuencia lo prueban?
- ¿Dónde se recuperarán los datos en caso de que ocurriese un desastre mayor en el centro de datos donde se alojan los sistemas de la compañía?

Adicionalmente se recomienda usar estos criterios para comparar las opciones de proveedor en nube antes de tomar una decisión:

- Certificaciones y estándares que cumple el proveedor
- Tecnologías usadas y servicios provistos
- Seguridad de datos, administración de datos y políticas del negocio
- Confiabilidad y rendimiento (detalle de las estadísticas sobre el cumplimiento de SLAs)
- Soporte de migración y planificación de salida (si se desea terminar el contrato y mover los sistemas a otro proveedor de nube)
- El proveedor debe ser una empresa estable que pueda continuar sus operaciones en el largo plazo.

9.2 Backup/Recovery Data Domain

Con el fin de que nuestra data sea parte del plan de continuidad del negocio se propone implementar un sistema de almacenamiento con deduplicación DELL EMC Data Domain, ya que resuelve muchos retos asociados con la copia de seguridad y replicación tradicional mediante la reducción de la cantidad de almacenamiento en disco necesario para conservar y proteger los datos. Utilizando esta tecnología se podrá lograr relaciones de reducción de espacio en disco de 10 a 30 veces más. Por lo tanto, los datos pueden ser retenidos en línea y en el lugar durante períodos más largo, por lo que restaurar ahora es más rápido y fiable.

9.2.1 Beneficios

Algunos de los beneficios más relevante de esta implementación son:

- Reducir los gastos de almacenamiento sin comprometer la protección de datos.
- La consolidación de más copias de seguridad en menos sistemas.
- Mitigar la necesidad de operaciones de TI en ubicaciones distribuidas
- Evitar los datos redundantes a partir de imágenes de disco de máquinas virtuales y facilitar virtualización de servidores
- Permite una replicación eficiente y cifrada en la red para la recuperación de desastres (DR).
- Replica solamente datos deduplicados y comprimidos sobre la red WAN lo que hace de esta operación económica y factible
- Reduce el costo total de propiedad (TCO) creando una estrategia de protección de datos basada en disco.
- Recuperar datos desde el disco mejora el tiempo de recuperación objetivo (RTO)
- Aumentar la frecuencia de copia de seguridad mejora el punto de recuperación objetivo (RPO)
- Aumenta las políticas de retención de datos y realizar recuperaciones de descubrimiento electrónico más eficazmente.

- Mejora la protección de datos y la productividad
- Mejora el rendimiento del sistema y la escalabilidad

9.2.2 Descripción de la solución

Esta solución nos brindara una combinación de alta velocidad y deduplicación en línea con compresión local, los sistemas Data Domain escriben solo datos únicos a disco. La tecnología de deduplicación reduce los requisitos de capacidad de disco y retrasos, mientras se incrementa la accesibilidad y la confianza.

La deduplicación segmenta el flujo de datos de entrada, únicamente identifica los segmentos de datos y luego compara estos segmentos a los datos previamente almacenado. Si un segmento de datos entrante es un duplicado de lo que ya está almacenado, este segmento no se almacena de nuevo, pero se crea una referencia al mismo. Si el segmento es único se almacena en el disco.

Detallamos factores fundamentales de los sistemas DELL EMC Data Domain:

- Verificación de extremo a extremo en el momento de la copia de seguridad: En esta área los datos se leen tal cual, para verificar que se trata de los datos correctos y que son accesibles a través del sistema de archivos hacia el disco. La mayoría de las restauraciones suceden dentro de un día o dos de los respaldos.
- Prevención y contención de fallas: Los nuevos datos nunca sobrescriben los datos correctos. Los sistemas Data Domain utilizan estructuras de datos menos complejas y memoria RAM volátil para el reinicio rápido y seguro. No se permiten estructuras parciales.
- Detección y reparación continuas de fallas: Data Domain RAID-6 proporciona protección de falla de disco y corrección de errores de lectura, detección y corrección de errores sobre la marcha, y limpieza para encontrar y reparar defectos crecientes en disco antes de que puedan convertirse en un problema
- Capacidad de recuperación del sistema de archivo: Los datos se escriben en un formato autodescriptivo. Si es necesario, el sistema de archivos puede

ser recreado escaneando el Log y reconstruyendo desde los metadatos almacenados con los datos.

- Deduplicación de alta velocidad: Reduce significativamente la capacidad de disco necesaria en el sistema, ya que solo los datos deduplicados se escriben en disco.
    - Altamente escalable para backup de largos periodos de retención
    - Reducción de datos promedio de 10 a 30 veces
    - Hasta 31 TB/hora de rendimiento agregado
- Rápido tiempo de preparación para la recuperación ante desastre: Como parte del proceso de deduplicación en línea, el sistema no tiene que esperar a escribir todo el conjunto de datos antes de que pueda comenzar a replicar al sitio remoto.
- Fácil integración: Soporta las principales soluciones de Backup, compatible con las principales aplicaciones empresariales
- Recuperación ante desastre rentable y multi sitio: Nos brinda una reducción de hasta el 99% del ancho de banda, proporciona topologías flexibles de replicación, replicación de hasta 270 sitios remotos.
- Almacenamiento ultra seguro para una recuperación confiable: La arquitectura de invulnerabilidad de datos proporciona verificación de recuperación continua, detección de fallas y curación, más un sistema de disco de paridad doble RAID-6
- Simplicidad operativa: reduce los costos administrativos, proporciona eficiencia en energía, enfriamiento y espacio para operaciones amigables con el medio ambiente, reduce la huella de hardware y es compatible con cualquier combinación de aplicaciones Backup y Archive en un solo sistema.

9.2.3 Esquema propuesto

El siguiente grafico muestra el esquema propuesto para la solución de Backup y Recovery para el centro de datos de la Unión compañía nacional de seguros, la misma que trae algunos componentes que se integran de manera nativa entre ellos.

Se instalarán los siguientes componentes:

- Data Domain Virtual Edition, Avamar & Recover Point for VM
    - Servidor Dell EMC PowerEdge R640
        - Data Domain Virtual Edition con capacidad de 4TB físicos (capacidad lógica aproximada de 40 TB – solo data estructura, no objetos, no archivos comprimidos)
        - Avamar Virtual Edition con capacidad de 4TB físicos
        - Recover Point for Virtual Machines con capacidad para 10 VMs
        - Data Protection Advisor
        - Data Protection Search
        - Data Protection Central
    - Servicio de Almacenamiento en Nube Privada
        - Replica diaria de respaldos hacia Nube Privada con la misma capacidad local

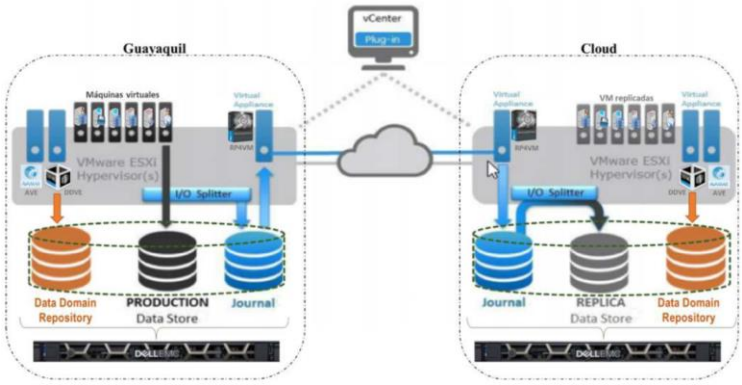
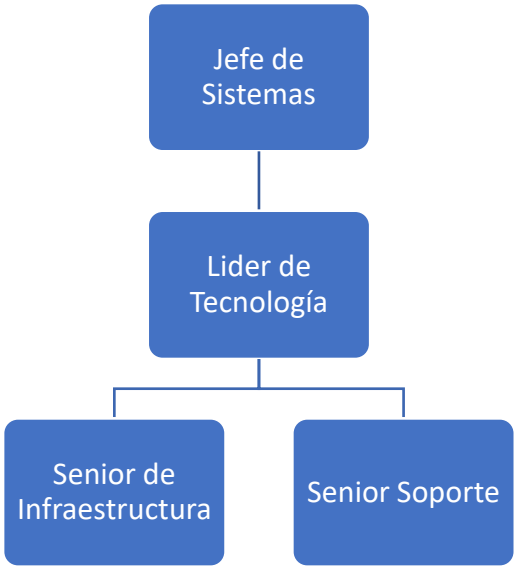


Figura 17: Esquema Data Domain
Fuente: Autor

9.3 Perfiles del personal de sistemas

En la auditoría realizada al departamento de sistemas y con base a las necesidades del giro del negocio, tendencias tecnológicas, y tendencias del mercado sugerimos que el organigrama del departamento quede distribuido de la siguiente manera:



Según el organigrama propuesto el jefe de sistemas y líder de operaciones son quienes estarán a cargo de las operaciones que sean necesarias dentro del centro de procesamiento de datos, y tomarán las decisiones y correctivos necesarios.

Se trabajará en conjunto con los asistentes Senior de Infraestructura y Senior Soporte para delegar tareas en caso de que se requiera.

10. Plan de respuesta y recuperación

10.1 Estrategias de recuperación

Una vez implementadas las soluciones propuestas en el documento definimos nuestro plan de recuperación y respuesta ante las amenazas externas e internas que inhabiliten la operación normal de nuestro centro de procesamiento de datos, toda ejecución de nuestro plan debe ser en un período de tiempo corto, para minimizar al máximo la interrupción.

10.2 Tipos de estrategias

Los tipos de estrategias a que vamos a ejecutar son realizados como medida de prevención y restauración de los procesos en el menor tiempo posible.

Las estrategias definidas son las siguientes:

Una vez implementadas las soluciones propuestas en el documento definimos nuestro plan de recuperación y respuesta ante las amenazas externas e internas que inhabiliten la operación normal de nuestro centro de procesamiento de datos, toda ejecución de nuestro plan debe ser en un período de tiempo corto, para minimizar al máximo la interrupción.

10.2.1 Backup

Son las copias de información que se realizan a los equipos del centro de procesamiento de datos, de modo que si ocurre un incidente que elimine, altere o modifique la integridad de los datos, poder tener la opción de regresar al punto anterior en la que las operaciones estaban normales.

Esto nos va ayudar significativamente ya que minimizamos las perdidas en el caso de que existan, y definitivamente tendremos un mejor tiempo de respuesta al momento de restablecer los equipos y recuperar la data después de un desastre.

10.2.2 Suministro de energía alterna

La compañía cuenta con un generador de energía que se activa si tenemos una interrupción, adicional contamos con un UPS que nos permite seguir operando con normalidad, mitigando el tiempo de suspensión de los servicios que ofrecemos.

10.2.3 Climatización

Contamos con un sistema de climatización centralizado, que permite que los equipos que se encuentran adentro del centro de procesamiento de datos funcionen con normalidad.

Adicional contamos con un aire acondicionado de respaldo en caso de que sea necesario por fallas del principal o mantenimiento.

10.2.4 Control de acceso físico

El control de acceso al centro de procesamiento de datos lo tenemos enfocado a un acceso con seguridad electrónica en la puerta de entrada de la oficina de sistemas al cual solo tiene acceso el personal del área de sistemas y adicional una puerta de vidrio templado que cuenta con una cerradura que se accede con una llave al cual solo tiene acceso el jefe de sistemas y el líder de tecnología. Y si algún proveedor o asistente de sistemas desea ingresar solo será con la debida autorización y compañía de las dos personas autorizadas.

El jefe de sistemas y líder de tecnología comparten una carpeta donde registran los accesos y las acciones realizadas en el centro de procesamiento de datos.

10.2.5 Monitoreo en tiempo real

El monitoreo está basado en mantener actualizado los documentos donde se registran los activos físicos y lógicos, los manuales de procesos y los cambios que se realicen, a dichos documentos solo tienen acceso el jefe de sistemas y el líder de tecnología, y pueden ser vistos desde cualquier lugar, con el fin de acceder a ellos y reaccionar de forma rápida y eficaz ante cualquier amenaza y así realizar las acciones correctivas o preventivas que se deseen.

10.2.6 Rediseño de red

El diseño de la red se implementó tal cual se lo propuso en la figura 17, ya que fue a corto plazo, nos ayudó significativamente segmentar la red creando las respectivas vlan.

Adicional contamos con redundancia en el servicio de internet con nuestro proveedor principal que nos brinda enlace de fibra y microonda, y nuestro proveedor secundario que nos brinda enlace de fibra.

10.2.7 Seguridad perimetral

Contamos con un firewall detallado en el documento proporcionado por nuestro proveedor principal de internet, el cual monitorea los ataques a los que estamos expuestos.

10.2.8 Sistema anti-spam

Contamos con un sistema anti-spam Avas Cloud E-mail Security proporcionado por nuestro proveedor principal de internet, el cual es monitoreado y gestionado por el líder de tecnología, con la finalidad de bloquear emails fraudulentos que perjudiquen la integridad, disponibilidad y confiabilidad de la data.

10.2.9 Extintor

En el departamento de sistemas se dispone de un extintor 95 BC – BIOXIDO DE CARBONO CO2 5 libras. en caso de algún evento de fuego que intente dañar los equipos del centro de procesamiento de datos.

10.3 Desarrollo de las estrategias

10.3.1 Backup

En base a lo establecido tenemos el detalle de la forma en la que se hacen los respaldos y como restablecer la información o sistema:

- Se realizan los respaldos tipo Snapshot de todas las máquinas virtuales de forma que la captura se realice con los últimos cambios realizados
- Los respaldos de las máquinas virtuales se realizan con las siguientes políticas.
    - Todos los días de modo incremental
    - Todos los días sábados se realiza un full backup
    - Política de retención de 7 días.
    - Los respaldos van secuenciales, es decir termina una maquina virtual y comienza la siguiente.

- Los respaldos de las máquinas virtuales se almacenan localmente en el centro de procesamiento de datos y en una nube privada contratada mediante nuestro proveedor del servicio Veeam.
- Los respaldos de los usuarios que se almacenan en el QNAP ubicado en el centro de procesamiento de datos, se replican en un NAS ubicado en el escritorio del líder de tecnología.
- Respaldo del servidor de correo se lo realiza semanalmente debido a que tenemos un sistema pop el cual descarga los emails en los terminales de los usuarios y los correos solo permanecen 15 días en el servidor y se lo ubica en las 3 ubicaciones QNAP, NAS y equipo del líder de tecnología.

10.3.2 Suministro de energía alterna

Ante un corte de suministro de energía automáticamente se realiza lo siguiente:

- El UPS que se encuentra adentro del centro de procesamiento de datos se activa automáticamente evitando que los equipos se apaguen.
- El generador se activa automáticamente y evita que el UPS se descargue por completo, evitando que exista una paralización en los servicios que ofrece la compañía.

10.3.3 Climatización

En el caso de que exista una falla en el aire acondicionado centralizado o se planifique algún mantenimiento en el mismo se realiza lo siguiente:

- El colaborador de sistemas indiferentemente del cargo tiene la obligación de encender el aire acondicionado de backup.

10.3.4 Control de acceso físico

El control de acceso al centro de procesamiento de datos se define de la siguiente manera:

- Tenemos implementada una cerradura con seguridad electrónica para acceder al departamento de sistemas con acceso restringido, solo el personal de sistemas puede ingresar o autorizar.
- El centro de procesamiento de datos cuenta con una cerradura de seguridad y su llave es responsabilidad del jefe de sistemas y líder de tecnología.
- El jefe de sistemas y líder de tecnología son las únicas personas autorizadas en ingresar o dar autorización y llevar un registro de ingreso.

10.3.5 Monitoreo en tiempo real

Se basa en los siguientes procedimientos:

- Los servidores físicos que alojan los servidores virtuales, cuentan con un sistema de alerta que funciona 24 horas todo el año que envía una notificación por correo al líder de tecnología en caso de alguna falla física o lógica solucionar inmediatamente.
- Adicional el líder de tecnología monitorea en tiempo real el funcionamiento del centro de procesamiento de datos mediante los diferentes portales de virtualización y redes.
- Se elabora un informe técnico en caso de que se presente una falla física o lógica en algún equipo y poder informar y tomar las respectivas soluciones.

10.3.6 Rediseño de red

Se verifica el correcto funcionamiento de la implementación del nuevo diseño de red asegurando la disponibilidad de la información:

- Se crearon las siguientes vlan:
    - Vlan de usuarios
    - Vlan de VoIP
    - Vlan de servidores
    - Vlan para red inalámbrica

- La segmentación ayudó a una mejora significativa en cuestión de disponibilidad.
- En caso de que nuestro enlace principal de fibra presente interrupciones automáticamente se activa el enlace microonda para evitar que la compañía deje de ejecutar sus operaciones.
- En caso de que la fibra y enlace microonda de nuestro proveedor principal fallen, el líder de tecnología es el encargado de realizar la conexión con el enlace de fibra de nuestro proveedor secundario a través de un router ya configurado.

10.3.7 SEGURIDAD PERIMETRAL

La seguridad perimetral es administrada actualmente por nuestro proveedor de internet principal, aunque se plantea contar con un firewall propio y configurarlo con las reglas y las políticas que requiera la compañía para su seguridad.

10.3.8 SISTEMA ANTI-SPAM

El líder de tecnología administra el Dashboard del sistema anti-spam Avas Cloud E-mail Security proporcionado por nuestro proveedor principal de internet donde se puede evidenciar:

- Destinatario del email
- Remitente del email
- Asusto
- Hora y fecha
- Estado del contenido:
    - Limpio
    - Spam
    - Cuarentena
- El líder de tecnología se encarga gestionar adecuadamente los dominios o email recibidos y enviarlos a:
    - Lista blanca
    - Lista negra

10.3.9 EXTINTOR

Cualquier colaborador del departamento de sistemas tiene la obligación de usar el extintor 95 BC – BIOXIDO DE CARBONO CO2 en caso de un evento de fuego que se presente en el centro de procesamiento de datos.

11. PROBAR PLAN DE RESPUESTA Y RECUPERACION

11.1 BACKUP

Se realiza una prueba de recuperación de una máquina virtual con la finalidad de obtener el tiempo exacto y con eso definimos un tiempo aproximado para las otras máquinas virtuales, el proceso es el mismo cuando se recupera desde el respaldo local y en la nube privada, mediante la herramienta Veeam Backup and Replication.

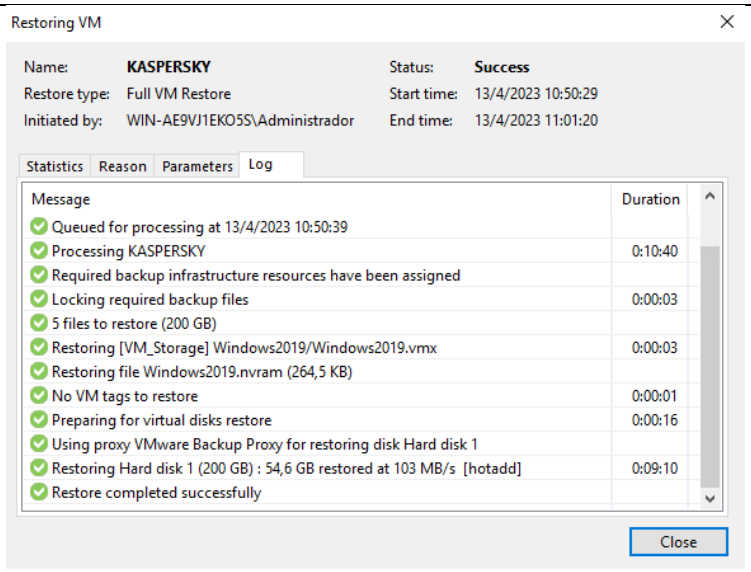


Figura 18: Proceso de restauración de un respaldo
Fuente: Autor

Podemos evidenciar que la restauración se realizó exitosamente con un tiempo de 9 minutos por una máquina virtual de 200 GB de almacenamiento.

En la figura 19 podemos evidenciar que la máquina virtual arrancó sin ningún inconveniente.

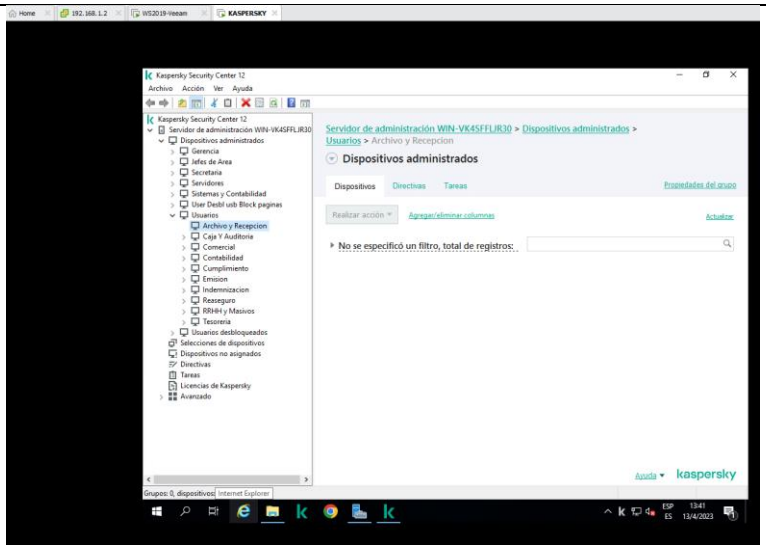


Figura 19: Evidencia de levantamiento del equipo
Fuente: Autor

11.2 Suministro de energía alterna

El centro de procesamiento de datos dispone de un UPS de 6 KVA para todos los equipos que se encuentran en el mismo, y adicional al momento de un corte de energía en la compañía se enciende el generador automáticamente.

Se realizó una medición cronometrada y se verifico que el generador de energía se activa a los 8 segundos aproximadamente, lo que ayuda a que el UPS no se descargue.

En el caso de que el generador de energía falle, se hizo una medición cronometrada y contamos con aproximadamente 15 minutos para apagar todas las máquinas virtuales y los equipos físicos para evitar inconvenientes.

De este proceso se encarga el jefe de sistemas junto al líder de tecnología.

11.3 Climatización

Una vez que se verifica que el aire acondicionado central no funciona, o si se realiza un mantenimiento programado, El control del aire acondicionado secundario se encuentra ubicado en el escritorio del líder de tecnología.

Y cualquier colaborador de sistemas tiene la obligación de encender el equipo sin ingresar al centro de procesamiento de datos para evitar sobrecalentamiento en los activos físicos presentes en el mismo.

11.4 Control de acceso físico

Solo el personal de sistemas tiene acceso al departamento mediante una cerradura electrónica, y adicional solo el jefe de sistemas y líder de tecnología tienen acceso al centro de procesamiento de datos y llenan una bitácora con los siguientes datos:

DIA	HORA ENTRADA	COLABORADOR	ACCIONES	HORA DE SALIDA
8/3/2023	9:00	JEFE DE SISTEMAS	VERIFICAR FUNCIONAMIENTO DEL SERVIDOR VEEAM	9:30
25/3/2023	14:00	LIDER DE TECNOLOGIA	CONEXIÓN DE CABLE DE RED A SWITCH DE RED INALAMBRICA	14:15
10/4/2023	18:00	LIDER DE TECNOLOGIA	REEMPLAZO DE MEMORIA RAM DEL SERVIDOR DELL POWEREDGE R640 IP 7	19:00

Tabla 19: Bitácora de ingreso a centro de procesamiento de datos
Fuente: Autor

11.5 Monitoreo en tiempo real

El líder de tecnología tiene configurado las alertas en los servidores para envíen notificaciones vía email ante cualquier evento de daño o actualización física y lógica.

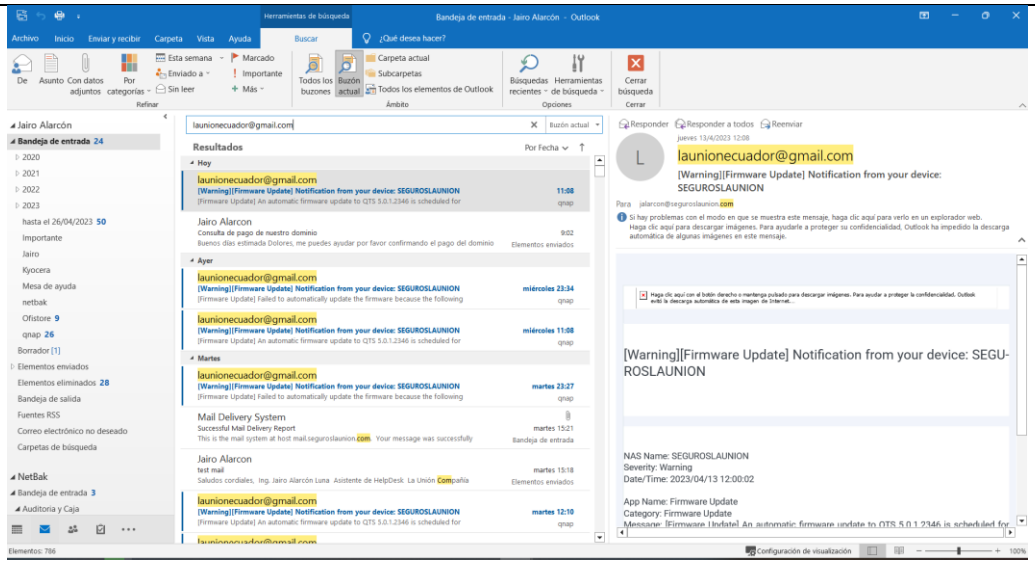


Figura 20: Evidencia de alertas de email
Fuente: Autor

Adicional se monitorea el funcionamiento de todos los servidores diariamente de forma manual para evidenciar si existe algún evento físico o lógico en los mismos.

Figura 21: Evidencia monitoreo de servidores
Fuente: Autor

11.6 Rediseño de red

Gracias al rediseño de red tenemos una mejor distribución en el direccionamiento ip para los equipos de la compañía.

Servidores: 192.168.1.x

Usuarios: 172.16.x.x

VoIP: 10.10.x.x

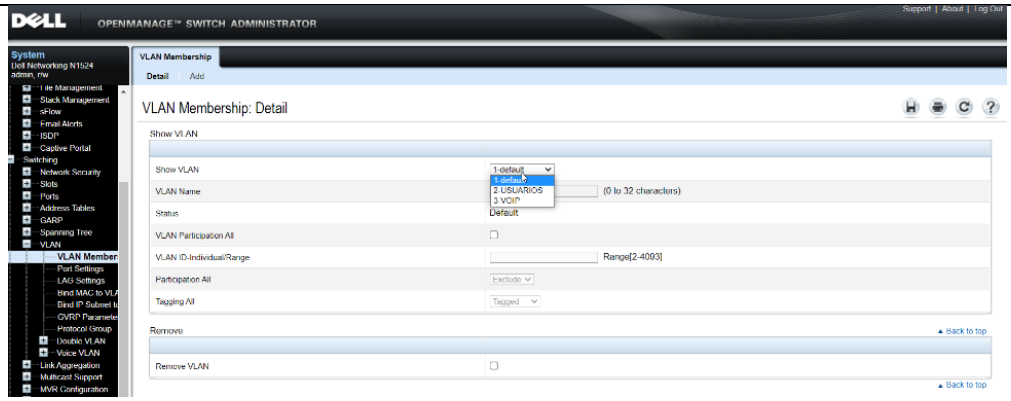


Figura 21: Vlan creadas
Fuente: Autor

11.7 Seguridad perimetral

Se debe solicitar un reporte a nuestro proveedor de los detalles de nuestra seguridad perimetral, y los ataques que presentamos para poder definir políticas internas.

11.8 Sistema Anti-spam

El líder de tecnología monitorea todos los días el Dashboard del sistema anti-spam que tenemos contratado con nuestro proveedor principal de internet

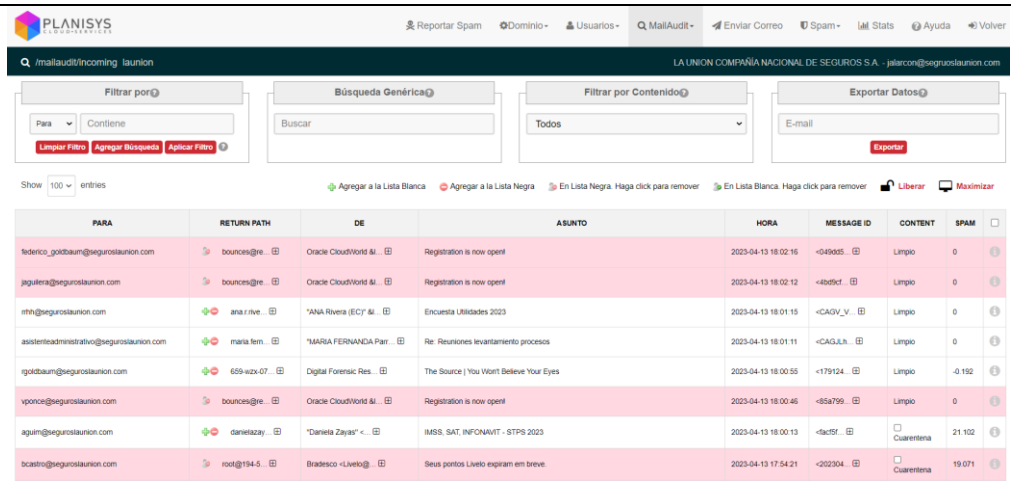


Figura 21: Dashboard del sistema anti-spam
Fuente: Autor

12. Políticas de seguridad

Con el fin de dar cumplimiento al plan de continuidad del negocio detallamos las políticas de seguridad que son necesarias para tener un ambiente seguro:

- Solo el personal autorizado ingresa al departamento de sistemas y al centro de procesamiento de datos.
- Mantener actualizada la bitácora con los registros de acceso al centro de procesamiento de datos.
- Revisar de forma periódica los registros de acceso, con la finalidad de verificar que se cumpla correctamente.
- Almacenar el registro de accesos durante un periodo de 5 años para depurar responsabilidades en caso de accesos indebidos
- Mantener actualizados los sistemas alojados en los equipos del centro de procesamiento de datos
- Se debe realizar cambio de contraseñas periódicamente y que tengan un grado de complejidad de longitud y uso de caracteres especiales.
- Realizar backup diario de las máquinas virtuales.
- Realizar pruebas periódicas de restauración de copias de seguridad para verificar su integridad.

- Realizar respaldo de la configuración de los equipos antes y después de realizar cambios.
- Mantener actualizada la base de firmas del antivirus Kaspersky y sincronizar los equipos.
- Realizar un Pentesting anual a los servidores de la compañía, y solucionar las vulnerabilidades encontradas.
- Monitorear constantemente la herramienta anti-spam que posee la compañía.
- Identificar los dispositivos conectados a nuestra red inalámbrica y bloquear a los que no están identificados.
- Realizar auditorias internas y externas al departamento de sistemas.
- Mantenimiento periódico de equipos del centro de procesamiento de datos
- Mantenimiento periódico al UPS 6KVA Online
- Elaborar plan de concientización de usuarios y ejecutarlo periódicamente
- Verificar contratos con proveedores de servicios
- Solicitar informes de estadísticas de nuestra seguridad perimetral a nuestro proveedor

13. MONITORIZACIÓN Y GESTIÓN

Una vez implementadas las salvaguardas y recomendaciones sugeridas se podrá realizar una gestión adecuada a la seguridad de nuestro centro de procesamiento de datos, y vamos a poder monitorear de manera eficiente y eficaz todo lo que sucede a nivel físico y lógico.

Se está documentando todos los procesos que se realizan el área de sistemas con el fin de definir responsabilidades y conocer el funcionamiento del centro de procesamiento de datos

Mediante la monitorización adecuada del centro de procesamiento de datos se puede detectar cualquier evento perjudicial, o incidencia y gestionarla inmediatamente.

14. Conclusiones y recomendaciones

El diseño de red actual presentaba inconvenientes debido a que era una red plana con un solo segmento, con la implementación de la propuesta a corto plazo se mejoró significativamente la distribución de red. Se recomienda llegar al esquema de red propuesto a largo plazo.

El diseño de respaldo era localmente, la data y los respaldos en el mismo centro de procesamiento de datos, con la implementación de la solución propuesta contamos con respaldo en la nube privada. Y respaldo en un equipo físico externo. Eso ayudo en la seguridad y tranquilidad de que los datos de la compañía están asegurados ante cualquier incidencia.

Algunos equipos actuales de comunicaciones con que cuenta la compañía pueden reutilizarse, aunque se recomienda adquirir equipos más actuales para llegar al esquema de red propuesto a largo plazo.

Si bien la implementación del nuevo diseño de red mejorará sustancialmente el rendimiento y seguridad de la re de la compañía, es importante también implementar una política de seguridad de la información alineada con la estrategia corporativa de la organización y que sea socializada entre los colaboradores de la compañía y cuyo cumplimiento sea medido a través de indicadores de un Sistema de Gestión de Seguridad Informática SGSI, tal y como se propone en las especificaciones de seguridad lógica del documento

Con el fin de que nuestra data sea parte del plan de continuidad del negocio se implementó un sistema de almacenamiento con deduplicación DELL EMC Data

Domain, ya que nos ayudó a resolver muchos retos asociados con la copia de seguridad y replicación tradicional mediante la reducción de la cantidad de almacenamiento en disco necesario para conservar y proteger los datos. Utilizando esta tecnología se logró relaciones de reducción de espacio en disco de 10 a 30 veces más. Por lo tanto, los datos pueden ser retenidos en línea y en el lugar durante períodos más largo, por lo que restaurar ahora es más rápido y fiable.

Implementar todas las salvaguardas sugeridas en el análisis de riesgos realizado con la metodología Magerit para reducir significativamente el impacto de los riesgos que tenemos actualmente en nuestro centro de procesamiento de datos.

Socializar nuestra política de seguridad a los miembros del departamento de sistemas, exponer el plan de continuidad del negocio a la gerencia y directorio para que evidencien cual sería la perdida cuantitativa si no se realiza lo sugerido en el plan.

Algunas de las recomendaciones sugeridas son:

- Implementar herramienta para notificación de ingresos lógicos a los equipos
- Implementar herramientas para monitoreo de red
- Implementar herramienta de análisis de software seguro
- Implementar el rediseño de red a largo plazo sugerido en el plan de continuidad del negocio
- Monitorear constantemente los respaldos.
- Implementar herramienta para seguridad de red inalámbrica
- Adquirir un Firewall con la finalidad de tener una protección perimetral propia de la compañía
- se sugiere realizar un cambio administrativo y definir el cargo basándose en los perfiles sugeridos para que pueda tener acceso total y documentar todos los procesos realizados con la debida autorización.

Referencias

ISO27000.ES, «Serie "27000",» [En línea]. Available: https://www.iso27000.es/iso27000.html. [Último acceso: 5 Enero 2022]

Instituto Nacional de Tecnologías de la Comunicación, «Implantación de un SGSI en la empresa,» [En línea]. Available: https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf. [Último acceso: 7 Enero 2022].

«Constitución de la República del Ecuador,» 25 Enero 2021. [En línea]. Available: https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/02/Constitucion-de-la-Republica-del-Ecuador_act_ene-2021.pdf. [Último acceso: 6 Enero 2022].

«Ley Orgánica de Protección de Datos Personales,» 26 Mayo 2021. [En línea]. Available: https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Ley-Organica-de-Datos- Personales.pdf. [Último acceso: 6 Enero 2022].

ISO27000.ES, «SGSI,» [En línea]. Available: https://www.iso27000.es/sgsi.html. [Último acceso: 5 Enero 2022].

«ISO 27001,» [En línea]. Available: https://normaiso27001.es/referencias-normativas-iso- 27000/#h31. [Último acceso: 6 Enero 2022].

MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. (s/f). Gob.es. Recuperado el 14 de abril de 2023, de https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

D. M. Alvarez Bernate, «Guía para la Elaboración de un Plan de Concientización y Entrenamiento, sobre Seguridad de la Información,» 2018

W. Mark y H. Joan, «NIST Special Publication 800-50,» 10 Enero 2022. [En línea]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf. [Último acceso: Octubre 2003].

Estándar NIST Special Publication 800-50:

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf

Juan A. Figueroa-Suarez (2017). La seguridad informática y la seguridad de la información. Ecuador

Martha R.C (2018). Introducción a la seguridad informática y el análisis de vulnerabilidades. Ecuador: Area de innovación y desarrollo S.L

2019, diciembre 11.¿Ques es la certificación ISO 27001 y para qué sirve?[Online]. Available: https://www.unir.net/ingenieria/revista/iso-27001/

Cesar H (2016). Amenazas Informáticas y Seguridad de la información

Arévalo Ascanio, J. G., Bayona Trillos, R. A., & Rico Bautista, D. W. (2015). Implantación de un sistema de gestión de seguridad de información bajo la ISO 27001: análisis del riesgo de la información

F. Silva, L. Segadas and E. Kwask "Gestión de la Seguridad de la Información" Colombia, RENATA, 2014, Julio.

2020 Septiembre 1.Las Herramientas de la seguridad de la informática para protegerán a tu empresa.

Ladino, M. I., Villa, P. A., & López, A. M. (2011). Fundamentos de ISO 27001 y su aplicación en las empresas. Scientia et technica, 17(47), 334-339.

ISO 27001 - Certificado ISO 27001 punto por punto - Presupuesto Online, 2013 [Online]. Available: https://normaiso27001.es/

A. Calder and S. Watkins and, "IT governance an international guide to data security and ISO 27001/ISO 27002".7th.ed. Kogan Page Publishers , 2012

Walter vega Velasco. (2008) Políticas Y Seguridad De La Información Enlace: http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2071-081X2008000100008

Port, D., Kazman, R. y Takenaka, A. (2008). Planificación estratégica para la seguridad y el aseguramiento de la información. Conferencia internacional de 2008 sobre seguridad y garantía de la información (isa 2008). Enlace: https://ieeexplore.ieee.org/document/4511612

Manual de sanciones por incumplimiento de política seguridad de la información (2020).

Enlace:https://www.scgg.gob.hn/sites/default/files/202002/Manual%20de%20Sanciones%20Final.pdf

Areitio, J. (2008). Seguridad de la información. Redes, informática y sistemas de información. España: Ediciones Paraninfo S.A.

INGERTEC , «Implantando ISO 27001 paso a paso - La Planificacion del SGSI,» INGERTEC , [En línea]. Available: https://normaiso27001.es/fase-4-planificacion-del-sgsi/. [Último acceso: 5 Agosto 2021].

Gobierno Electrónico de Ecuador, GUÍA PARA LA GESTIÓN DE RIESGOS DE SEGURIDADD DE LA INFORMACIÓN, Quito: Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2020.

C. A. G. SILVA, diseño de un sistema de gestion de seguridad de la información para una entidad financiera, Bogotá: INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO , 2015.

J. A. GARZÓN RODRÍGUEZ y J. F. SÁNCHEZ ESCOBAR, diseño de un sistema de gestión de seguridad de la información para el proceso de gestión comercial de la empresa jre ingeniería con base en la norma iso 27001:2013, bogotá: universidad piloto de colombia, 2020.

F. J. Valencia Duque y M. Orozco Alzate, Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000, Manizales: Revista lbérica de Sistemas y Tecnologías de Información, 2017.

PMG SSI , «Norma 27001 2013,» PMG SSI , 08 Mayo 2020. [En línea]. Available: https://www.pmg-ssi.com/norma-27001/. [Último acceso: 05 Agosto 2021].

F. L. LANDETA GUACHAMIN y D. F. QUILLE SIMBAÑA, análisis y diseño de un sistema de gestión de seguridad de la información en base a las normas iso 27001 y 27002 para la superintendencia de control del poder de mercado., quito: Universidad Politécnica Salesiana, 2016

Andreu, F. I. (2006). REDES WLAN, Fundamentos y aplicaciones de seguridad. España: Marcombo S.A.

Tanenbaum, A. W. (2012). Redes de computadoras (Vol. Quinta Edición). Estado de México: Pearson.

CAUBIT, R.; BASTOS, A. ISO 27001 e 27002 – Uma visão prática. Editora Zouk, 2009.

DIAS, C. Segurança e auditoria da tecnologia da informação. Axcel Books, 2000.

FONTES, E. Políticas e Normas para a Segurança da Informação. Bras- port, 2012.

ICONTEC. Compendio Sistema de Gestión de la Seguridad de la Información (SGSI), segunda ed., 2009.

Flavia Esteslia Silva Coelho, L. G. (2015). Gestion de la seguridad de la informacion . Bogota.

Huguet, M. C., Arques, J. M., & Galindo , E. M. (2008). Administracion de sistemas operativos en red. Barcelona.

Vieites, A. G. (2014). Enciclopedia de seguridad informatico. Madrid.

G. Altares, «El País,» 18 02 2021. [En línea]. Available: https://elpais.com/cultura/2021-02-17/el-ignorado-espia-que-le-hizo-ganar-la-guerra-a-stalin.html. [Último acceso: 03 08 2021].

ISOTools, «ISOTools.org,» [En línea]. Available: https://www.isotools.org/.

O. Fonseca, MODELO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA ORGANIZACIÓN GEOCONSULT CS, Bogotá, 2019.

P. Sulliva, «Tech Target,» 22 11 2016. [En línea]. Available: https://searchdatacenter.techtarget.com/es/consejo/Gestion-de-riesgos-de-seguridad-de-la-informacion-Comprension-de-los-componentes. [Último acceso: 04 08 2021].

ISO 22301 Gestión de Continuidad de Negocio. (n.d.). Bsigroup.com. Retrieved April 14, 2023, from https://www.bsigroup.com/es-ES/ISO-22301-continuidad-de-negocio/

ISO 22301 Continuidad del Negocio. (s/f). Normas ISO. Recuperado el 14 de abril de 2023, de https://www.normas-iso.com/iso-22301-continuidad-del-negocio/

Certificación ISO 22301 - Norma de continuidad del negocio. (s/f). Nqa.com. Recuperado el 14 de abril de 2023, de https://www.nqa.com/es-pe/certification/standards/iso-22301

ISO 22301. (2013, diciembre 10). Software ISO. https://www.isotools.us/normas/riesgos-y-seguridad/iso-22301/