ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"CERTIFICACIÓN DEL PROCESO DE MONITOREO DEL BACKBONE DE DATOS Y SERVICIOS CLOUD BAJO LA NORMA ISO 27001:2013 EN UNA EMPRESA DEL SECTOR DE TELECOMUNICACIONES CONSIDERANDO LOS ACTIVOS A CARGA DEL ÁREA DE TRANSPORTE DE DATOS."

EXAMEN DE GRADO (COMPLEXIVO)

PREVIO A LA OBTENCIÓN DEL TÍTULO DE

MAGÍSTER EN SISTEMAS DE INFORMACIÓNGERENCIAL

AUTOR:

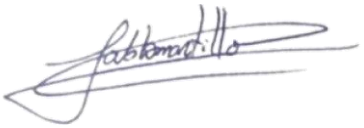
PABLO ANDRÉS MARTILLO CAMPOVERDE

GUAYAQUIL – ECUADOR

AÑO: 2021

AGRADECIMIENTO

Agradezco a Dios por la salud que ha permitido a mi familia gozar durante esta época de pandemia y a mi familia que me ha apoyado e incentivado a cumplir las metas que me he propuesto y a seguir creciendo en lo profesional y lo personal.



DEDICATORIA

Dedico este trabajo a:

A mi esposa Adriana quien me ha acompañado a lo largo de toda mi carrera como estudiante universitario desde el pregrado, su afecto y apoyo me brindan fuerzas para mejorar cada día. A mis padres quienes me han enseñado el valor de las cosas y me han brindado su apoyo, conocimientos y amor para poder progresar en esta etapa de mi vida.

TRIBUNAL DE SUSTENTACIÓN

MSIG. Lenin Freire Cobo
COORDINADOR MSIG

MSIG. Juan Carlos García
PROFESOR MSIG

RESUMEN

Este trabajo presenta la participación del área de trasporte de datos y seguridades en la certificación del proceso de monitoreo del backbone de datos y servicios cloud bajo la norma ISO 27001:2013, lo que permite a la empresa competir en el mercado de servicios en la nube, que se encuentra en crecimiento en el Ecuador, brindando garantías a nivel de seguridad de la información a sus clientes y potenciales clientes.

En una empresa de telecomunicaciones, habitualmente dedicada al negocio de telefonía móvil, telefonía fija y servicios de internet, se ha planteado incursionar en nuevas tendencias del mercado como son el Internet de las cosas (IOT), servicios en la nube, entre otros. Para esto existe un proceso de transformar sus instalaciones que anteriormente eran conocidas como “centrales”, donde el espacio físico era exclusivo para equipos que brindan sus servicios tradicionales, en centros de datos (Datacenter) que permitan albergar servidores que puedan ser utilizados no solo para la propia empresa sino para vender servicios a sus clientes.

Para garantizar la correcta operación de estos centros de datos y brindar tranquilidad a los clientes de que se cuenta con espacios físicos adecuados y

personal capacitado para atender el mismo, se requieren de cumplir con ciertos estándares y normas. La norma ISO 27001 es una estándar internacional que permite asegurar la confidencialidad, integridad y disponibilidad de la información. La certificación bajo la norma ISO 27001:2013 refleja hacia los clientes el cuidado que tiene la empresa sobre la información que el cliente está proporcionando como son los datos y servicios que aloje en los dispositivos de la compañía.

La seguridad de la información cada día toma mayor importancia ya que el número de ataques informáticos va en aumento. Es importante para la empresa poder certificar que sus procedimientos, dispositivos y personal siguen las normas internacionales indicadas en la ISO 27001. Una correcta aplicación de la norma puede evitar pérdidas económicas, bajar participación en el mercado y daños a la imagen pública para nuestros clientes.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

COIP	Código Orgánico Integral Penal
IOT	Internet of Things – Internet de las cosas
ISO	International Organization for Standardization
M2M	Machine to Machine – Máquina a Máquina
NTP	Network Time Protocol – Protocolo de sincronización de reloj
O&M	Operación y Mantenimiento
SGSI	Sistema de Gestión de Seguridad de la Información
SOA	Statement of Aplicability – Declaración de aplicabilidad
TI	Tecnología de Información
VRF	Virtual Routing and Forwanding

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

La empresa de telecomunicaciones se encuentra operando en Ecuador desde hace más de 25 años, iniciándose con el servicio de voz y datos móviles donde cada año tuvo que ir adaptándose a nuevas tecnologías existentes con redes 2G, 3G y 4G. Posteriormente fue incluyendo en su portafolio servicios de voz, internet y televisión para el segmento de hogar; sin embargo, las empresas de este sector no pueden detenerse y deben seguir evolucionando hacia nuevas soluciones. Por esta situación, desde el año 2010 ha venido trabajando fuertemente en el segmento corporativo, brindando servicios de internet y enlaces de datos para los clientes. La empresa ha utilizado la infraestructura ya desplegada previamente para los servicios móviles en todo el Ecuador.

Una vez que la empresa ha logrado obtener participación en el mercado de clientes corporativos, desde el año 2015 empieza un proceso de transformación de las instalaciones conocidas como centrales de la empresa para convertirlas en centro de datos que permitan alojar servicios de nuestros clientes en las mismas instalaciones. Realizan adecuaciones físicas y se preparan nuevos procedimientos y personal para la atención de los nuevos centros de datos.

Los centros de datos han pasado por procesos de certificación en su diseño y operación, pero esto no es suficiente para asegurar a los clientes corporativos que estamos preparados para contar con sus servicios e información en nuestros equipos. El incremento en los números de ataques informáticos es un factor clave para decidir dónde los clientes pueden colocar su información, ya que se registra un aumento del 56% en ataques de informáticos a empresas públicas en todo el mundo durante el año 2021. [1]

Preocupados por esta realidad en el año 2019 se empezó un proyecto para obtener una certificación en seguridad de la información del transporte y monitoreo de los servicios en la nube, logrando en el año 2021 obtener la certificación ISO 27001:2013, que indica que la empresa trabaja con normas internacionales para garantizar disponibilidad, integridad y confidencialidad de los servicios en la nube que administra.

El presente trabajo está enfocado en la participación que tuvo el área encargada de la operación y mantenimiento de los equipos de transporte de datos sobre el proceso de certificación, mismo que se encuentra dividido en 3 capítulos cuyos resúmenes se muestran continuación:

- El primer capítulo describe la problemática actual que está teniendo la compañía en la implementación de servicios en la nube, los motivos para obtener una certificación en seguridad de la información y los objetivos que se esperan alcanzar al finalizar el proceso.

- El segundo capítulo nos muestra el proceso de aplicación de la norma ISO 27001. Se especifican los conceptos claves como son los activos, riesgos y controles, y se detalla la implementación realizada por el área de transporte de datos de la compañía.

- En el tercer capítulo se muestran los procesos de auditoría interna y externa realizados para poder obtener la certificación. Los correctivos que se tuvieron que tomar en base a las novedades encontrados por el equipo auditor y el resultado final del proceso de certificación.

CAPÍTULO 1

GENERALIDADES

1.1 ANTECEDENTES

La empresa del sector de telecomunicaciones lleva más de 25 años en el país, empezando con servicios de telefonía celular y pasando por transiciones hasta contar en su portafolio con servicios para segmentos de hogar y corporativo. En el sector corporativo los estudios de mercado han demostrado que la empresa está por debajo de al menos 3 de sus directos competidores.

Por esto desde el año 2010 la empresa tomó la decisión estratégica de incrementar esfuerzos por recuperar el espacio perdido en el mercado

corporativo para obtener mayores ganancias. En la actualidad estos trabajos han llevado a la compañía a contar con más de 800 clientes corporativos con diferentes servicios (internet, enlaces dedicados, M2M). Posteriormente la evolución de la tecnología y la adaptación de la empresa a esta evolución ha permitido brindar a los clientes servicios en la nube.

1.2 DESCRIPCIÓN DEL PROBLEMA

Como parte del crecimiento de la empresa en el área de las telecomunicaciones se han implementado centros de datos con el objetivo de obtener un nuevo nicho de mercado. Sin embargo, el mercado actual ya tiene varios competidores y para poder ingresar al mismo la empresa ha invertido en certificaciones para que sus centros de datos puedan estar a la altura de aquellos que posee la competencia.

Los clientes de servicios de cómputo en la nube cada vez se han vuelto más exigentes y conscientes de lo expuesto que queda su información al no estar alojada en sus propios servidores. Por lo cual requieren tener una certeza de que la empresa se preocupa por la seguridad de la información que maneja. En Ecuador los líderes en el mercado de servicios en la nube poseen certificaciones que permiten a sus clientes conocer que sus procesos adoptan las mejores prácticas para proteger la información, por

lo cual se ha dificultado el crecimiento de este producto para la empresa ya que se encuentra en desventaja con respecto a los líderes del mercado.

Las políticas de seguridad de la información en la compañía no han sido revisadas en los últimos 5 años, teniendo algunos procedimientos que deben ser mejorados, listado de los equipos desactualizados y personal que no es consciente de la importancia de la seguridad de la información en sus operaciones.

1.3 SOLUCIÓN PROPUESTA

La norma ISO 27001 es uno de los estándares más reconocidos para la protección de la seguridad de la información, brindando un marco que permite garantizar la confidencialidad, integridad y disponibilidad de los activos de la información siendo estos personas, equipos y procesos de la compañía.

Lograr obtener la certificación bajo la norma ISO27001:2013 permite a la empresa poder competir con los líderes del mercado de productos en la nube. Dado que este requerimiento es puntual para los servicios en la nube, el alcance de la certificación se limita al proceso de “Monitoreo del backbone de datos y servicios cloud”, de modo que se pueda garantizar

que todos activos involucrados en este proceso cumplen con los estándares solicitados por la ISO27001.

La certificación requiere implementar un Sistema de Gestión de Seguridad de la Información (SGSI), comenzando con un análisis de los activos participantes del proceso, y a partir de estos identificar los riesgos asociados a los mismos y los controles a implementar para que estos riesgos no sean explotados por atacantes generando un impacto en la organización.

Dentro del proceso de certificación intervienen varias áreas de la empresa, todas ellas lideradas por el área de seguridad de la información quienes son los responsables de obtener la certificación. El presente trabajo se centra en las actividades realizadas por el área encargada del transporte de datos, detallando la participación sobre los activos relacionados al área que permitieron alcanzar la certificación.

1.4 OBJETIVO GENERAL

- Obtener la certificación del proceso de monitoreo del backbone de datos y servicios cloud bajo la norma ISO 27001:2013, lo que permite a la compañía competir con sus similares en el mercado de servicios en la nube.

1.5 OBJETIVOS ESPECÍFICOS

- Identificar los riesgos asociados a los activos del área de transporte de datos.
- Validar los controles existentes para evitar que los riesgos puedan ser explotados.
- Implementar acciones correctivas y mejoras en procedimientos que permitan asegurar la información.
- Realizar auditoría interna y externa de las acciones realizadas para obtener la certificación a nivel internacional.

CAPÍTULO 2

APLICACIÓN ISO 27001

2.1 NORMA ISO 27001

El estándar o norma ISO/IEC 27001 contiene una serie de requisitos que debe cumplir el sistema de gestión de seguridad de la información (SGSI) de las empresas que desean certificarse. Es un documento con requerimientos generales y aplicables a todo tipo de organizaciones. En caso de no aplicar algún control para el alcance del SGSI se debe justificar su incumplimiento. Esta norma fue publicada en octubre del año 2005, su certificación dura 3 años y es realizada por entidades externas que han sido previamente avaladas para realizar las auditorias de los SGSI. Para

obtener la certificación es necesario pasar por las fases mostradas en la **figura 2.1**. [2]

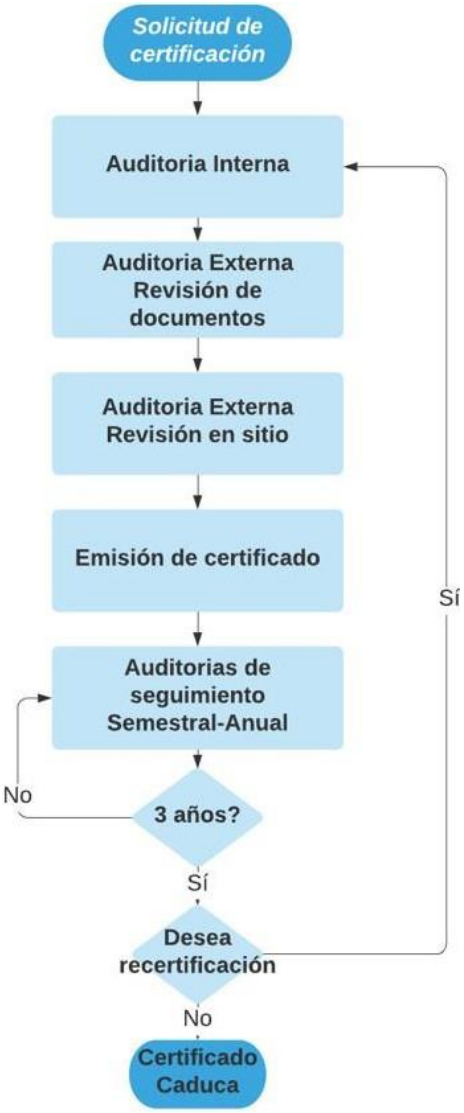


FIGURA 2.1 PROCESO DE CERTIFICACIÓN
Fuente: ISO27000.ES

El SGSI es el documento que contiene las políticas que seguirá la empresa para garantizar la confidencialidad, integridad y disponibilidad de la información que administra. Estos son los 3 pilares principales que debe implementar un SGSI, aunque dependiendo del contexto de la empresa podría extenderse hacia nuevas características de la seguridad de la información como autenticidad, no repudio, trazabilidad, entre otros. [3]

- **Confidencialidad:** La información es únicamente accesible y visible para las personas autorizadas. Previene que la misma sea divulgada a personal no autorizado.

- **Integridad:** La información no puede ser alterada en ninguna circunstancia, sin que exista una autorización previa del responsable de esta.

- **Disponibilidad:** La información se encuentra disponible para las personas autorizadas en todo momento que la necesiten. Debe prevenirse interrupciones en el acceso a la información.

La norma ISO 27001, para considerar una correcta implementación, indica que el SGSI debe contar con 2 secciones:

- **Requerimientos:** Se encuentran enumerados del 0 al 10, y es mandatorio cumplir con los puntos del 4 al 10 para lograr la certificación. El SGSI debe especificar:

    - Alcance
    - Liderazgo – Política
    - Planificación
    - Soporte
    - Operación
    - Evaluación del desempeño
    - Mejora

- **Controles:** Se encuentran definidos en el Anexo A de la norma ISO 27001 y contiene 14 dominios con 35 objetivos de control y 114 controles. La norma no obliga que se cumplan todos los controles ni tiene definidos controles obligatorios, la implementación de cada control dependerá de la evaluación de riesgo realizada por la empresa.

2.2 CONTEXTO DE LA ORGANIZACIÓN

La norma ISO 27001 nos indica que debemos comprender el contexto de la organización, identificando los factores externos e internos que intervienen en la gestión del riesgo, alcance del SGSI y los criterios para la evaluación del riesgo. Conocer la organización nos permite lograr los resultados esperados en la implementación del SGSI. Para esto se debe analizar 3 aspectos de la organización y el equipo de trabajo se ha servido de ciertas herramientas que se presentan en la **tabla 1**.

TABLA 1. HERRAMIENTAS PARA ANALIZAR ASPECTOS DE LA ORGANIZACIÓN

Fuente: Autor

Aspecto	Herramientas
Definir objetivos del negocio y resultados esperados del SGSI.	Misión, Visión, Objetivos, Valores, Finalidad del SGSI.
Analizar factores externos que puedan afectar los resultados.	Análisis PEST.
Analizar factores internos que puedan afectar los resultados.	Análisis FODA.

La empresa posee definida su misión, visión, objetivos y valores que fueron a su vez revisados y plasmados en el documento formal del SGSI. Se tuvo

una reunión entre la presidencia, los directores y gerentes de cada área para durante un taller definir la finalidad que se acerque más a las expectativas de la compañía acerca del SGSI, delimitando el alcance y conociendo las partes interesadas en el proyecto.

El análisis PEST es una herramienta que permite hacer una investigación del entorno de la compañía mediante el análisis de factores cuyas iniciales componen el nombre del análisis. Se analizan los factores Políticos, Económicos, Sociales y Tecnológicos que están presentes en el entorno en el que opera la empresa y que permiten definir las nuevas tendencias y la estrategia empresarial. [4]

Entre los talleres realizados, se lograron identificar algunos puntos como parte del análisis PEST entre los que resaltan los indicados en la **figura 2.2**.

FIGURA 2.2 ANÁLISIS PEST DE LA COMPAÑÍA
Fuente: Autor

El análisis FODA viene de las siglas Fortalezas, Oportunidades, Debilidades y Amenazas. Mientras que la herramienta de análisis PEST permitió realizar un análisis del contorno de la empresa centrados en un enfoque externo, el FODA permite evaluar al proyecto de certificación directamente y las variables que permitirán lograr su éxito desde un enfoque interior de la empresa.

Los principales elementos encontrados durante el análisis FODA se detallan en la **figura 2.3**.

FIGURA 2.3 ANÁLISIS FODA DEL PROCESO
Fuente: Autor

2.3 ALCANCE DEL SGSI

El alcance del SGSI es el punto de partida para prepararse para la certificación bajo la norma ISO 27001. El alcance permite identificar los límites del SGSI y para esto se deben considerar 3 factores acorde a la norma:

- Asuntos externos e internos.
- Requisitos de las partes interesadas.
- Procesos y actividades con otras organizaciones.

Los asuntos externos e internos en torno a la compañía y el proceso de certificación fueron revisados dentro del contexto con los análisis PEST y FODA. Los resultados de los análisis han permitido a la empresa realizar un enfoque en dos productos claves para el negocio como son la transmisión de datos y servicios en la nube.

Las partes interesadas son aquellas personas u organizaciones que puedan resultar afectadas, involucradas o participar en el proceso de certificación. Es importante para el SGSI conocer cuáles son las partes interesadas y cuáles son sus requerimientos. Por esto se elabora la **tabla 2** con las principales partes interesadas del proceso de certificación.

TABLA 2. PARTES INTERESADAS

Fuente: Autor

Parte interesada	**Necesidad**	**Expectativa**
Cliente corporativo	• Garantía de que su información está a salvo. • Proveedores certificados por norma.	Certificación ISO27001:2013

Departamento Comercial	• Crecimiento en soluciones TI. • Igualar a la competencia.	Creación de soluciones garantizando la seguridad de la información.
Departamento de Marketing	• Crear estrategia de mercado promocionando seguridad de la información.	Promocionar la certificación obtenida con los clientes corporativos
Departamento de TI	• Garantizar que sus procesos, equipos y personal cumplen la norma.	Superar las auditorias y corregir los controles para obtener la certificación
Gobierno	• Cumplir de directrices gubernamentales. • Cumplir políticas de telecomunicaciones.	Encontrar auditorias de cumplimiento periódicas

Luego de estas consideraciones se debe elaborar el alcance, el cual debe tener los siguientes componentes:

- Servicios y/o Productos: Backbone de datos y servicios cloud.
- Procesos y/o Actividades: Monitoreo
- Ubicaciones: Quito y Guayaquil

El alcance de la certificación del SGSI de la compañía será:

“Monitoreo del backbone de datos y servicios cloud en Quito y Guayaquil”

2.4 ACTIVOS DE LA INFORMACIÓN

El siguiente paso en la preparación para obtener la certificación bajo la norma ISO27001 del SGSI implementado en la empresa, fue identificar los activos de la información que forman parte del alcance definido para el SGSI.

Un activo de información es un elemento necesario para que un proceso de negocio se pueda desarrollar. Posee valor para la empresa y se debe cuidar la información que contiene o cursa por el mismo en sus tres propiedades: confidencialidad, integridad y disponibilidad. Para el SGSI los

activos relevantes son aquellos que dan soporte al alcance previamente definido.

Se han definido tres categorías para la clasificación de los activos que a su vez los siguientes tipos de activos:

- **Entorno**
  - **Instalaciones**: edificios, oficinas, centros de datos, entre otros.
  - **Equipos y Suministros**: dispositivos de red, cableado, suministros de energía, entre otros.
  - **Personal**: Empleados asociados a su cargo en la compañía. Ej: Director, Gerente, Operativo, etc.

- **Equipos de computo**
  - **Hardware**: PCs, Laptop, teléfonos inteligentes.
  - **Base de datos**: Repositorios con datos que provean información relevante al proyecto.
  - **Sistemas Operativos**: Conjunto de programas y configuraciones de equipos como PC, servidores, enrutadores.

- **Sistemas de información**
    - **Aplicaciones**: Software utilizado para las actividades del proceso.
    - **Datos**: Documentos físicos o digitales con información acerca de la empresa.

Se realizó la clasificación de los activos relacionadas a cada área participante en el proceso de certificación del SGSI, definiendo el dueño del activo, la persona responsable del mismo y que puede delegar su administración, y el custodio del activo, quien se encarga de la administración o utilización del activo. En el presente documento se presentarán únicamente información acerca de los activos del área de operación y mantenimiento del transporte de datos.

Para poder representar los activos involucrados es importante conocer la topología de red a nivel macro que posee la empresa, donde existen 4 enrutadores centrales que son el “backbone” de la red. Por estos 4 equipos pasan todos los servicios de la compañía por esto fueron los escogidos para la certificación junto con los equipos que brindan soporte a los servicios en la nube, mismos que no serán detallados en el presente documento. La topología de la red de forma general se presenta en la **figura 2.4**.

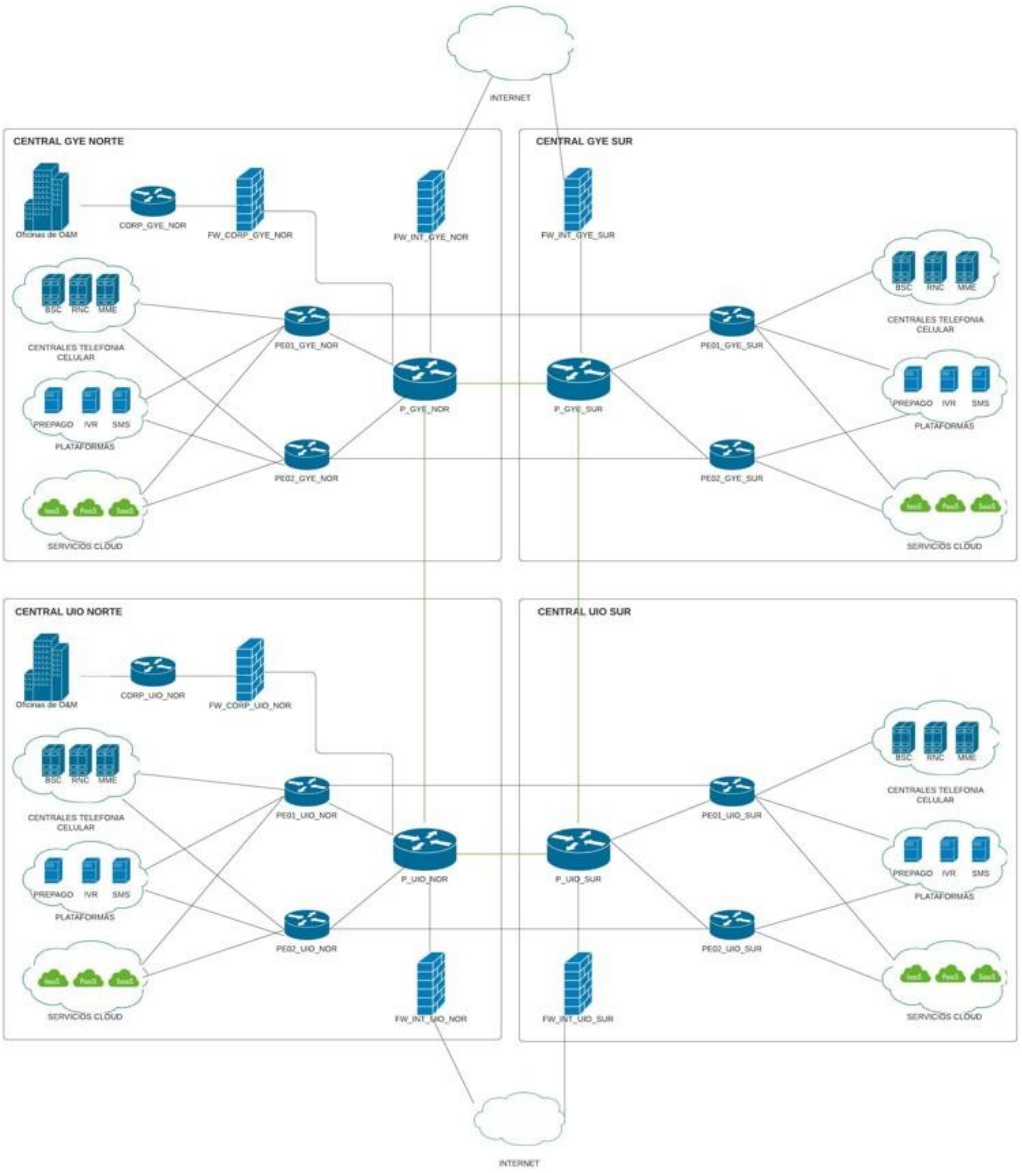


FIGURA 2.4 TOPOLOGIA DE RED DE LA EMPRESA
Fuente: Autor

Los activos descritos en el **anexo A** son los identificados por parte del área de operación y mantenimiento (O&M) para el proceso de certificación ISO 27001.

2.5 RIESGOS

Existen algunos términos que se deben describir antes de entrar en la definición de riesgo, estos son las amenazas y vulnerabilidades. Todos los activos poseen vulnerabilidades que es una falla o debilidad presente en el activo, ya sea este un equipo, tecnología, proceso o persona. Una amenaza es todo lo que presente una intención de realizar un daño a un activo.

El riesgo es la posibilidad de que una amenaza pueda explotar una vulnerabilidad de un equipo, generando un impacto en la organización. El impacto son las consecuencias que sufre la empresa luego de que sus activos han sido afectados. Dado que todos los activos poseen vulnerabilidades, a su vez poseen un riesgo inherente asociado al mismo. Estos riesgos deben ser identificados para prevenir que las amenazas logren su propósito de afectar a la organización.

El proceso de identificar los riesgos de cada activo tiene los siguientes pasos:

1. Identificar amenazas hacia el activo.
2. Conocer las vulnerabilidades del activo.
3. Determinar las consecuencias de que la vulnerabilidad se explote.
4. Especificar el riesgo.

Una vez identificado los riesgos se debe realizar un análisis y clasificación de estos, ya que se debe priorizar la atención a aquellos con un nivel de riesgo más alto. Existen 2 variables que nos permitirán hacer un análisis de riesgos, la probabilidad de que un evento ocurra y el impacto que tendrá el mismo una vez que suceda. Cada variable se calificará entre 5 niveles: Muy Baja, Baja, Media, Alta y Muy Alta. El cruce de estas 2 variables nos permitirá obtener un nivel del riesgo acorde a lo mostrado en la **figura 2.5**.

FIGURA 2.5 VALORACIÓN DEL NIVEL DE RIESGO
Fuente: Enredando Proyectos [5]

Para la identificación de los riesgos asociados a cada activo, el comité de seguridad tuvo reuniones individuales con cada una de las áreas participantes y que poseen activos dentro del proceso. En las reuniones se aclaraba el uso del activo, el impacto en caso de daño de este y las contingencias que se poseen para evitar que un evento suceda; estos parámetros sirven para definir la probabilidad de que el riesgo se

materialice. El resultado de los riesgos asociados a cada activo se presenta en el **Anexo B**; dado que se poseen activos similares, pero en distintas ubicaciones físicas, se los ha agrupado para la presentación.

2.6 CONTROLES

Luego de identificados los riesgos asociados a cada activo es necesario especificar los controles existentes o que están por implementarse para prevenir los eventos que afecten a la seguridad de la información. El control es una acción que es tomada por la empresa y que pueden ser de forma preventiva, detectiva o correctiva.

- Preventiva: Nos ayuda a evitar los eventos que puedan aprovechar el riesgo.
- Detectiva: Sirve para identificar la existencia de un evento sobre un activo de información.
- Correctiva: Minimiza los impactos cuando se ha presentado un evento de seguridad.

Cuando ya se ha identificado los controles aplicados sobre los riesgos existentes de los equipos, es necesario evaluar nuevamente el riesgo luego de que se cuenta con el control, esto se conoce como riesgo residual

y también debe ser medido su nivel de riesgo para determinar si es un valor aceptable. La **figura 2.6** explica el proceso de identificación que se ha tenido a raíz de los activos de la información para realizar un análisis de riesgo.

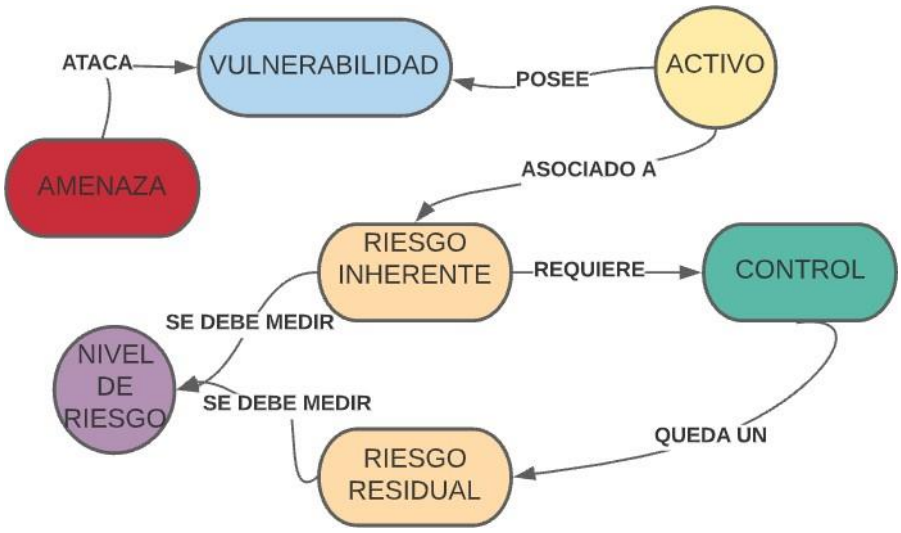


FIGURA 2.6 ANÁLISIS DEL RIESGO
Fuente: Autor

La norma ISO 27001 en su anexo A posee 14 dominios de seguridad, 35 objetivos de control y 114 controles. En la **tabla 3** se presenta un ejemplo de uno de los dominios de seguridad, donde el dominio de seguridad es la categoría principal (A6), que a su vez tiene 2 objetivos de control (6.1 y 6.2) con 7 controles.

TABLA 3. EJEMPLO DE DOMINIO DE SEGURIDAD

Fuente: Autor

A6	**Organización de la seguridad de la información**	
A6.1	**Organización interna**	
A.6.1.1	Roles y responsabilidades en seguridad de la información	Se debe definir y asignar todas las responsabilidades de la seguridad de la información.
A.6.1.2	Segregación de tareas	Tareas o áreas de responsabilidad en conflicto deben ser segregadas para reducir las oportunidades de modificación no autorizada o involuntaria o el uso inadecuado de los activos de la organización.
A.6.1.3	Contacto con las autoridades	Se debe mantener contacto adecuado con las autoridades respectivas
A.6.1.4	Contacto con grupos de interés especial	Deben mantenerse los contactos apropiados con grupos de interés especial, u otros foros y asociaciones profesionales especializados en seguridad.
A.6.1.5	Seguridad de la información en la gestión de proyectos	La seguridad de la información debe adaptarse a la gestión del proyecto, independientemente del tipo de proyecto.
A6.2	**Los dispositivos móviles y el teletrabajo**	
A.6.2.1	Política de dispositivos móviles	Se debe adoptar políticas y medidas de soporte de seguridad para el manejo de los riesgos derivados del uso de equipos móviles.
A.6.2.2	Teletrabajo	Se debe implementar políticas y medidas de soporte de seguridad para proteger la información a la que se accede, procesa o almacena en los lugares de trabajo a distancia.

En base al listado de controles de la norma ISO27001 se han logrado encontrar aquellos que logran reducir el riesgo identificado previamente para los activos de interés de la certificación y se los presenta en el **Anexo C.**

2.7 PLAN DE TRATAMIENTO

El plan de tratamiento son las acciones que se realizarán con el riesgo residual que ha sido calculado luego de aplicar los controles elegidos. Existen 4 opciones principales para el tratamiento del riesgo residual:

- Evitar: Retirar, eliminar o suspender las actividades que causan el riesgo.

- Mitigar: Tomar medidas para la reducción de la probabilidad de ocurrencia del riesgo o que permitan minimizar el impacto en caso de ocurrir.

- Transferir: Realizar actividades que permitan que la responsabilidad del riesgo sea manejada por un tercero.

- Asumir: Cuando se decide no tomar ninguna acción sobre el riesgo y aceptar el mismo. Solo es aconsejable cuando se tiene un nivel bajo de riesgo residual.

Para los riesgos identificados en los activos se han definido las siguientes opciones y acciones como parte del plan de tratamiento, éstos se detallan en el **Anexo D**.

2.8 CONTROLES CRÍTICOS

Hasta ahora se ha revisado en base a los riesgos de los activos, cuales controles debemos aplicar para prevenir que las amenazas se lleguen a materializar; sin embargo, existen controles críticos que son transversales para la compañía y que deben ser cumplidos por todas las áreas sobre sus activos de la información. Para estos controles se debe presentar una justificación en caso de no implementarlos.

Se realizó una revisión con el comité de seguridad y las gerencias involucradas en el proyecto para definir las exclusiones y aquellos controles sobre los que si se debe presentar soporte. A continuación, se resaltan los más relevante para el área de transporte de datos.

- **A.9.2.4 - Gestión de la información secreta de autenticación de los usuarios**

La norma indica que “se debe controlar la asignación de la información de autenticación secreta de usuarios mediante un proceso de gestión formal”. Para esto la empresa posee normado en el manual TI-091 que las claves de los usuarios se las obtiene mediante un portal de autoservicio, de tal modo que la única persona que puede conocer la clave es el usuario final. Un ejemplo del portal se muestra en la **figura 2.7**.

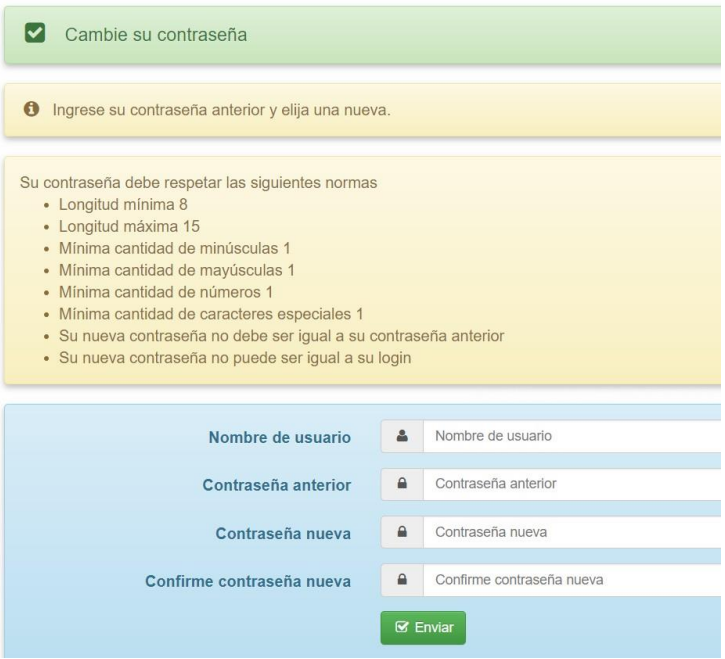
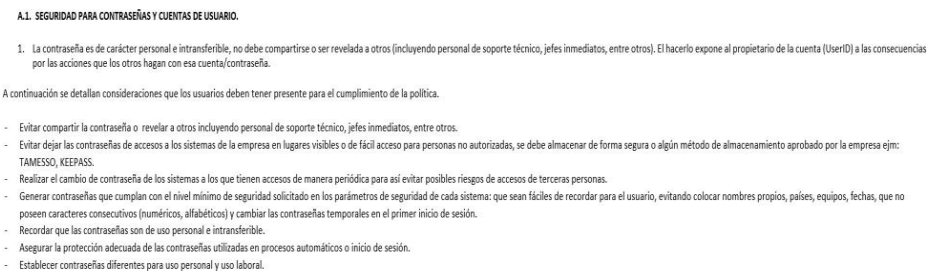


FIGURA 2.7 SISTEMA DE GESTION DE CONTRASEÑAS

Fuente: Autor

- **A.9.3.1 - Uso de la información secreta de autenticación**

La compañía posee procedimientos claros sobre el uso de las contraseñas y consideraciones para cumplir la política. Estos son recordados constantemente por el departamento de seguridad y la gerente de O&M. Se presenta un extracto del correo con las consideraciones en la **figura 2.8.**



A.1. SEGURIDAD PARA CONTRASEÑAS Y CUENTAS DE USUARIO.

1. La contraseña es de carácter personal e intransferible, no debe compartirse o ser revelada a otros (incluyendo personal de soporte técnico, jefes inmediatos, entre otros). El hacerlo expone al propietario de la cuenta (UserID) a las consecuencias por las acciones que los otros hagan con esa cuenta/contraseña.

A continuación se detallan consideraciones que los usuarios deben tener presente para el cumplimiento de la política.

- Evitar compartir la contraseña o revelar a otros incluyendo personal de soporte técnico, jefes inmediatos, entre otros.
- Evitar dejar las contraseñas de accesos a los sistemas de la empresa en lugares visibles o de fácil acceso para personas no autorizadas, se debe almacenar de forma segura o algún método de almacenamiento aprobado por la empresa ejm: TAMESSO, KEEPASS.
- Realizar el cambio de contraseña de los sistemas a los que tienen accesos de manera periódica para así evitar posibles riesgos de accesos de terceras personas.
- Generar contraseñas que cumplan con el nivel mínimo de seguridad solicitado en los parámetros de seguridad de cada sistema: que sean fáciles de recordar para el usuario, evitando colocar nombres propios, países, equipos, fechas, que no poseen caracteres consecutivos (numéricos, alfabéticos) y cambiar las contraseñas temporales en el primer inicio de sesión.
- Recordar que las contraseñas son de uso personal e intransferible.
- Asegurar la protección adecuada de las contraseñas utilizadas en procesos automáticos o inicio de sesión.
- Establecer contraseñas diferentes para uso personal y uso laboral.

FIGURA 2.8 CORREO DE NOTIFICACIÓN DE MANEJO DE CLAVES

Fuente: Autor

- **A.11.2.5 - Retirada de materiales propiedad de la empresa**

El procedimiento para el retiro de los materiales de la empresa actualmente es mediante un correo electrónico a la consola de seguridad para que le permita ya sea a personal interno o externo el retiro de un activo de la empresa. El correo debe detallar:

- Nombre del activo a retirar
- Descripción del activo
- Número de serie
- Destino
- Motivo
- Personal que retira
- Autorización del dueño o custodio del activo

- **A.12.4.4 – Sincronización del reloj**

  La norma exige que todos los equipos que son parte de la organización o al menos aquellos que son parte del dominio de seguridad del SGSI tengan una sola fuente de donde se sincronice el tiempo del reloj. Esto ayuda a tener precisión al momento de relacionar eventos entre los diversos activos del SGSI.

  De forma general la compañía posee una sola fuente satelital para la sincronización del reloj, junto con varios servidores NTP para distribuir la carga; sin embargo, todos los servidores NTP se sincronizan con la misma fuente satelital.

- **A.13.1.2 - Seguridad de los servicios de red**

En este control, la norma solicita identificar mecanismos de control de la seguridad de los servicios de red. Para esto la empresa cuenta con el manual TI-072 que nos indica que todas las solicitudes de acceso a redes deben ser solicitadas mediante el portal SST. Las redes de usuarios finales con las redes de las plataformas y dispositivos se encuentran separadas por “firewalls” y para poder permitir el acceso se requiere que el usuario ingrese una solicitud en el portal SST, caso contrario la comunicación será bloqueada. También se definen las aprobaciones por la que debe pasar la solicitud antes de ser configurada. En la **figura 2.9** se presenta un flujo de las aprobaciones por la que atraviesa la solicitud de un usuario.

Fecha y Hora	Estado	Comentarios	Grupo	Tiempos
2017-08-01 15:33:23	Solicitada		Solicitantes	
2017-08-04 15:41:51	Aprobada	Acceso a reportes y KPIs de I2000 Plataforma One AMX	Jefe Inmediato	3 dias, 0 horas, 08 minutos
2017-08-04 15:44:40	Aprobada	ok	Administrador de Activo Tecnologico	0 dias, 0 horas, 02 minutos
2017-08-04 17:42:59	Aprobada	proceder	Jefe Back Office Datos	0 dias, 1 horas, 58 minutos
2017-08-08 12:30:54	Ejecutada	Ejecutado	Ing. de BackOffice Datos	3 dias, 18 horas, 47 minutos

FIGURA 2.9 FLUJO DE APROBACIONES DE UNA SOLICITUD

Fuente: Autor

- **A.13.1.3 – Segregación en redes**

Se deben separar los diferentes servicios entre ellos, así como de los usuarios y sistemas de información. La segregación de las redes existe en la compañía, donde se separan los servicios mediante el uso de VRFs que permiten tener distintas redes virtuales coexistiendo dentro de una misma topología y a los usuarios colocando un “firewall” intermedio para brindar mayor seguridad. Utilizando el diagrama de red se puede evidenciar la segregación de redes que se tiene mediante el uso de VRFs y Firewalls para una de las centrales, esto se demuestra en la **figura 2.10**.

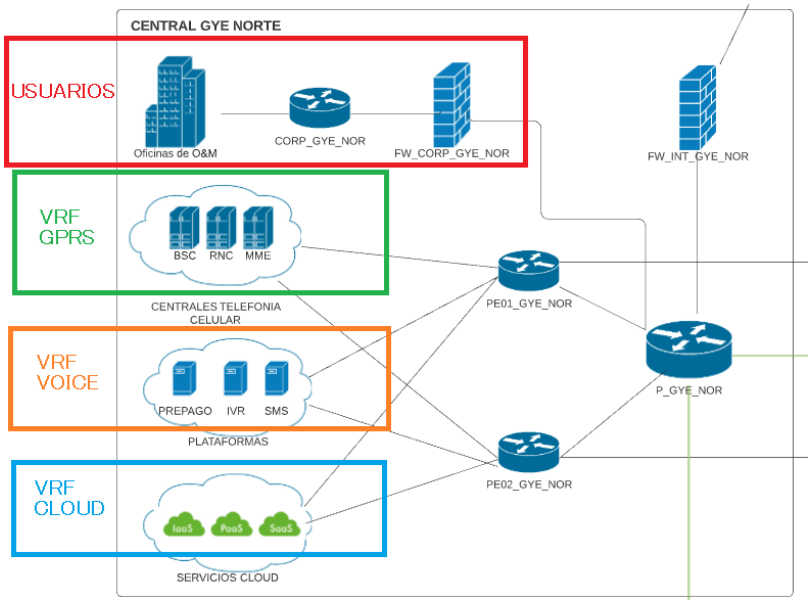


FIGURA 2.10 SEGMENTACIÓN DE REDES

Fuente: Autor

Finalmente, todos los controles implementados, tanto aquellos determinados en base a los riesgos como los controles críticos son colocados en un solo documento llamado SoA o declaración de aplicabilidad. El documento SoA tiene como finalidad indicar aquellos controles que se han aplicado dentro del alcance del SGSI y justificar aquellos controles del Anexo A de la norma ISO 27001 que han sido excluidos. Este es uno de los documentos vitales para la auditoría del SGSI.

CAPÍTULO 3

AUDITORÍAS Y RESULTADOS

3.1 AUDITORÍA INTERNA

La empresa posee un área de auditorías que responde directamente a la presidencia de la compañía. Mientras se realizaban los ajustes al SGSI, se trabajó en la certificación de personal del área de auditoría como auditores internos bajo la norma ISO27001:2013. De este modo al ser un ente externo al proceso de desarrollo del SGSI nos permite evaluar la correcta implementación de este y prepararnos para la auditoría externa de certificación del proceso.

El proceso de auditoría interna tomó 2 meses para la revisión del SoA. A continuación, se detallan los hallazgos encontrados por los auditores internos:

- **Publicación de manuales a partes externas (proveedores)**

  Durante el proceso de implementación del SGSI se han realizado actualizaciones a varios manuales de la compañía y muchos de ellos son de importancia para los proveedores. Se encontró que la notificación de los cambios fue realizada a la interna de la compañía, pero no fue notificada en el portal de proveedores.

  Se realizó las correcciones para mantener actualizado el portal de proveedores con los manuales relevantes para cada proveedor.

- **Existencia de roles en el SGSI que no corresponden a cargos en la compañía**

  Se pudo evidenciar roles presentes en el SGSI sin que quede claro el personal de la compañía que estará a cargo de esas funciones. Los roles eran de “oficial de seguridad de la información” y “coordinador de seguridad de la información”.

Se elimina el rol de “oficial de seguridad de la información” del SGSI para evitar confusiones y se define el cargo de “jefe de seguridad informática” como el rol de “coordinador de seguridad de la información”.

- **Matriz de riesgos contiene error en tipo de plan de tratamiento para 2 controles.**

  Dentro de la matriz de riesgos, para 2 controles se ha aplicado el mismo plan de tratamiento, pero en el tipo se ha seleccionado “Transferir” para un plan de acción y “Mitigar” para el otro.

  Esto es un error en el tipeo ya que al ser un mismo plan de acción no pueden ser de 2 tipos distintos. Se corrige el documento de la matriz de riesgos, la opción correcta era “Mitigar”.

- **No existe listado de grupos de interés**

  Los grupos de interés son las personas interesadas del proyecto de certificación, pese a que se elaboró un listado durante las sesiones de trabajos, el mismo no fue almacenado debido a la rotación del

personal y de proveedores. En base a esta observación se realiza un listado considerando solo los cargos de las personas interesadas y los principales proveedores.

- **Implementación de control A.12.3.1**

Para el área de transporte de datos este control no fue considerado, sin embargo, en las revisiones realizadas con auditoría se encontró útil incluir este control. El control A.12.3.1 se refiere a las copias de seguridad de los equipos, a pesar de que esto está incluido en el plan de continuidad de la información se lo agrega como un control sobre los enrutadores.

Los enrutadores poseen configuraciones que son respaldadas todos los días por un sistema interno llamado PHOENIX. Estos respaldos son almacenados por 30 días, para que puedan ser usados en caso de algún inconveniente con el dispositivo como pérdida de información o daño del equipo. Se demuestra al auditor que se cumple con las copias de seguridad y se agrega al SoA el control sugerido. En la **figura 3.1** se muestra el sistema que se utiliza para los respaldos de configuración de los enrutadores.

FIGURA 3.1 SISTEMA DE RESPALDOS PHOENIX

Fuente: Autor

- **Indicadores de controles de red**

Durante la reunión con auditoría se solicitó realizar un control de indicadores sobre los controles en el acceso a las redes. Dado que esto está implementado dentro de un portal llamado SST, resulta fácil hacer un control mensual de la cantidad de solicitudes atendidas y rechazadas. Se implementa el indicador y se establece compromiso para la realización mensual del mismo, mostrado en la **figura 3.2**.

ESTADO	Solicitu	Fecha creacion	Fecha Modificacio	Estado	Tipo	Tipo Solicitud	Tipo Permis	Fecha Vencimient
EJECUTADAS	4487	22/9/2020 18:22	28/9/2020 13:03	Ejecutada	Personal	Firewall	Permanente	
EJECUTADAS	4435	15/9/2020 9:49	15/9/2020 14:22	Ejecutada	Personal	Firewall	Permanente	
EJECUTADAS	4384	8/9/2020 10:32	8/9/2020 16:46	Ejecutada	Personal	Firewall	Temporal	30/11/2020
EJECUTADAS	4361	3/9/2020 17:36	4/9/2020 12:05	Ejecutada	Personal	Firewall	Temporal	3/12/2020
EJECUTADAS	4325	31/8/2020 11:16	7/9/2020 12:08	Ejecutada	Proveedor	Firewall	Permanente	
EJECUTADAS	4568	30/9/2020 9:59	30/9/2020 18:32	Ejecutada	Personal	Firewall	Temporal	21/12/2020
EJECUTADAS	4507	23/9/2020 19:24	24/9/2020 17:27	Ejecutada	Personal	Firewall	Permanente	
EJECUTADAS	4428	14/9/2020 9:55	15/9/2020 12:45	Ejecutada	Personal	Firewall	Permanente	
EJECUTADAS	4385	8/9/2020 9:03	10/9/2020 17:45	Ejecutada	Personal	Firewall	Permanente	
EJECUTADAS	4350	2/9/2020 16:23	3/9/2020 8:37	Ejecutada	Personal	Firewall	Temporal	30/9/2021
EJECUTADAS	4347	2/9/2020 13:42	3/9/2020 7:12	Ejecutada	Personal	Firewall	Temporal	30/11/2020
EJECUTADAS	4345	2/9/2020 11:10	7/9/2020 11:24	Ejecutada	Proveedor	Firewall	Permanente	
EJECUTADAS	4328	31/8/2020 14:38	2/9/2020 7:44	Ejecutada	Personal	Firewall	Permanente	
EJECUTADAS	4552	28/9/2020 15:47	29/9/2020 8:41	Ejecutada	Proveedor	Firewall	Permanente	
EJECUTADAS	4505	23/9/2020 15:53	24/9/2020 9:44	Ejecutada	Personal	Firewall	Permanente	
EJECUTADAS	4468	18/9/2020 17:14	18/9/2020 17:52	Ejecutada	Personal	Firewall	Temporal	30/9/2020
EJECUTADAS	4419	11/9/2020 16:08	15/9/2020 13:17	Ejecutada	Personal	Firewall	Permanente	
EJECUTADAS	4411	10/9/2020 15:59	11/9/2020 16:07	Ejecutada	Personal	Firewall	Permanente	
EJECUTADAS	4370	7/9/2020 15:55	8/9/2020 15:15	Ejecutada	Personal	Firewall	Temporal	30/9/2020
EJECUTADAS	4268	25/8/2020 16:52	4/9/2020 11:16	Ejecutada	Personal	VPN Remote Access	Permanente	
RECHAZADAS	4426	11/9/2020 18:40	15/9/2020 9:41	Rechazada	Personal	Firewall	Permanente	
RECHAZADAS	4359	3/9/2020 16:32	3/9/2020 17:28	Rechazada	Personal	Firewall	Temporal	3/12/2020
RECHAZADAS	4562	29/9/2020 12:54	30/9/2020 9:53	Rechazada	Proveedor	VPN Remote Access	Temporal	21/12/2020
RECHAZADAS	4422	11/9/2020 17:22	15/9/2020 13:05	Rechazada	Personal	Firewall	Permanente	

FIGURA 3.2 INFORME DE SOLICITUDES ATENDIDAS MENSUALMENTE

Fuente Autor

Una vez realizadas las correcciones o mejores planteadas por el equipo de auditoría dentro de la auditoría interna, se procede a enviar los documentos a la entidad certificadora para empezar el proceso de certificación.

3.2 AUDITORÍA EXTERNA

Para que el SGSI de la empresa pueda presentarse a una entidad de certificación debe tener una existencia demostrable de al menos 3 meses. Todas las entidades de certificación deben ofrecer un mismo número de jornadas de auditorías a pesar de que sus costos puedan variar. Una vez

escogida la entidad de certificación el siguiente paso es establecer un contacto inicial donde se reúnen los auditores designados con el comité de seguridad para desarrollar el plan de auditoría y establecer las fechas de esta. [2]

Las auditorías poseen 2 fases, la primera no es requerida que sea en sitio dado que se trata de revisión de documentos mientras que la segunda fase suele ser en sitio para entender la documentación y verificar los controles. Para el caso de la empresa, debido a la pandemia sufrida por el COVID 19, ambas fases fueron realizadas de forma remota, brindando facilidades al ente certificador para mostrar las instalaciones, personal y dispositivos a través de video llamada.

La primera fase requiere que el comité de seguridad envíe a los auditores la documentación del SGSI junto con los manuales y procedimientos definidos como soporte para los controles implementados, así como el documento SoA. Esta fase no puede durar más de 6 meses, para el caso de la empresa esta fase tomo alrededor de 3 meses.

La segunda fase requiere que el auditor comprenda las operaciones de los procesos involucrados en el alcance del SGSI, por lo que empieza a tener reuniones tanto con personal de seguridad de la información, líderes del proyecto, como con todas las áreas involucradas. Con cada área los auditores tienen como mínimo 2 sesiones de 4 horas para poder aclarar sus ideas sobre los activos y el proceso para luego poder solicitar los soportes que consideren necesarios.

La fase 2 finaliza con un informe de auditoría que contiene un resultado del proceso de certificación, no conformidades encontradas y fechas que dispone el auditado para cumplir con las correcciones a las no conformidades encontradas. Las no conformidades se pueden clasificar en mayores y menores, dependiendo de esto será la urgencia de tomar una acción correctiva que pueda ser revisada por el auditor.

Para las no conformidades es necesario establecer un plan de acción que evite su repetición en una próxima auditoría y un análisis de causa raíz para determinar los factores que han llevado a tener esta no conformidad.

Durante las reuniones con el área de O&M se pudo evidenciar las siguientes novedades:

- **Sobre el control de acceso a las instalaciones**

  En el proceso que tenemos personal de la compañía cuenta con sus credenciales para acceso mediante lectores a la entrada de cada cuarto de la central o departamento, sin embargo, para los visitantes se entrega en garita una tarjeta temporal identificada con la etiqueta “VISITANTE” y el nombre del proveedor.

  El auditor recomienda que esta tarjeta debe ser visible durante el tiempo que el visitante esté dentro de las instalaciones, sean central u oficinas, para que cualquier personal de la compañía pueda supervisar las actividades realizadas por personal externo y reportar en caso de encontrar en alguna actividad sospechosa.

  Se presenta como una oportunidad mejora, pero no es registrado como una no conformidad por parte del auditor. Dado que estas tarjetas son administradas por el área de seguridad física, se escala a la gerencia la novedad indicada para tomar acciones.

- **Sobre la eliminación de soportes y retiro de materiales**

  Se demostró el procedimiento actual, considerando un caso existente de un activo cuyo disco duro se averió y se tuvo que aplicar cambio por parte del proveedor. Se mostró la evidencia de la gestión de acceso y el correo donde el jefe de transporte de datos autoriza al jefe de datacenter para que permita el retiro del disco duro averiado al proveedor.

  También se demostró la evidencia de que el proveedor realizó la destrucción física del disco duro averiado acorde al contrato de confidencialidad que se posee con el mismo.

  Sin embargo, como no conformidad en este proceso se solicitó que en casos de retiros de elementos que contengan información exista una notificación explicita de que el elemento NO posee información sensible.

  Para esta recomendación como primer paso se agrega en el manual TI-007 un párrafo indicando que el jefe de transporte de datos debe indicar en el correo al jefe de datacenter que el elemento que se va a retirar no contiene información sensible junto con los demás datos

que identifican al activo. El siguiente paso será incluir un campo en el portal de ingreso a centrales una opción para marcar si el elemento posee o no información sensible.

- **Sobre los respaldos de los activos**

  El auditor observa los respaldos generados para los 4 enrutadores involucrados y nota que en efecto se está almacenando los mismos por un mes. Lo que solicita es una validación de integridad para garantizar que los archivos presentes en la herramienta PHOENIX corresponden al equipo.

  Se realiza un documento de validación de integridad para cada uno de los routers, generando un respaldo en la herramienta PHOENIX y descargando en un archivo de texto. A la vez se realiza la descarga de las configuraciones actuales del enrutador. Para la comparación se utiliza el programa Notepad++ que posee una herramienta para comparar archivos de texto. De aquí se demuestra al auditor que el contenido del respaldo es el mismo que las configuraciones actuales como se observa en la **figura 3.3**.

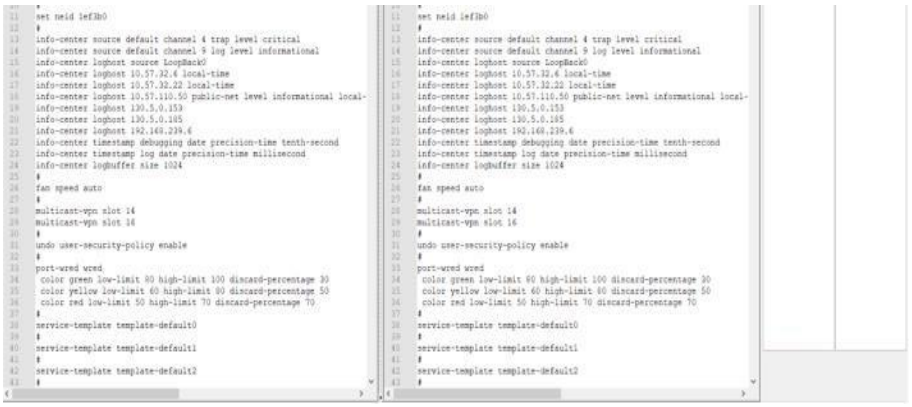


FIGURA 3.3 VALIDACIÓN DE INTEGRIDAD DE UN ENRUTADOR

Fuente: Autor

Sobre los respaldos de los enrutadores también indicó que el control A.12.3.1 requiere que se realice la restauración de los respaldos generados. Sobre este punto se presentó una “no conformidad” sobre la que se detalla en la sección 3.2.1 de no conformidades.

3.2.1 NO CONFORMIDADES

En la reunión de cierre del proceso de auditoría se identificaron 8 no conformidades en el proceso a certificar, de las cuales 7 fueron menores y una mayor. Para las no conformidades menores el auditor brindó un tiempo de 90 días como plazo máximo para tomar los correctivos mientras que para la no conformidad mayor se otorgó un tiempo máximo de 30 días para presentar los correctivos. Los resultados se muestran resumidos en la **tabla 4**.

TABLA 4. NO CONFORMIDADES

Fuente Autor

TIPO	PROCESO	ÁREA	OBSERVACIÓN
Menor	Gestión de auditoría interna	Auditoría	No se cumplió con las fechas previstas del plan de auditoría.
Menor	Gestión de auditoría interna	Auditoría	No se valida la efectividad de las acciones tomadas en el plan de tratamiento.
Menor	Normalización de procesos	Procesos	El sistema de almacenamiento de documentos sufre afectación y se pierde acceso durante la auditoría.

			Se debe considerar este sistema como crítico para el SGSI.
Mayor	Normalización de procesos	Procesos	Existen inconsistencias entre las versiones de documentos presentados. Los cambios no pueden ser validados y no se presentan soportes debido a la falla del sistema de almacenamiento.
Menor	Herramienta de documentación	Administrativo	Análisis de nivel de riesgo no evidencia la realidad, ya que se ha definido un fallo en la herramienta de documentación con un nivel bajo, pero al presentarse se observa problemas para obtener los documentos.
Menor	Selección de personal	Talento humano	La norma pide la revisión de antecedentes penales sin embargo se indica que en Ecuador las leyes no permiten realizar esta validación durante el proceso de selección.

Menor	Retiro de activos	O&M	Se solicita que exista una notificación formal de que el activo que se está retirando posee o no posee información sensible.
Menor	Respaldo de información	O&M	No se está realizando pruebas de restauración. Se debe realizar una prueba de restauración de los respaldos obtenidos en forma periódica.

Para el análisis de causa raíz de las no conformidades se utilizó la herramienta de “los 5 por qué” que consiste en realizar 5 preguntas relacionadas con la no conformidad para evitar que vuelva a suceder. A continuación, se presentará el análisis realizado para las 2 no conformidades correspondientes al área de O&M transporte de datos.

- **Retiro de activos**
  - Análisis causa raíz.

Problemática: En el requerimiento de retiro de hardware que se solicita gestionar al Ingeniero de datacenter no se especifica si el disco duro contiene información sensible

1. **¿Por qué no se realiza la notificación de que el disco posee información sensible?** En el alcance de la ISO27001 se especificó que los enrutadores no manejan información sensible.

2. **¿Por qué los enrutadores no almacenan información sensible?** Son dispositivos que lo único que almacenan son las configuraciones para su funcionamiento.

3. **¿Por qué no hay riesgo si se obtiene la configuración del enrutador?** No representa un riesgo para la empresa ya que no tiene información de clientes ni de la compañía, mientras una persona no tenga acceso no puede realizar modificaciones sobre el enrutador.

4. **¿Por qué la configuración no posee información sobre las redes de la empresa?** El intercambio de las rutas se realiza en otros enrutadores, en el backbone solo realizan tránsito.

5. **¿Por qué es útil la recomendación de especificar la existencia de información sensible?** Permite realizar un análisis nuevamente y verificar si hay algún tipo de información sensible remanente en los equipos.

- **Plan de acción**: Se implementará un campo obligatorio en el sistema de tickets donde se debe especificar la existencia o no de información sensible en el activo que se está manipulando.

- **Resultado**: Luego de 25 días de levantada la novedad se desarrollan campos para identificar si los activos contienen información sensible o no. Estos campos son obligatorios para generar el ticket hacia el departamento de Datacenter como se muestra en la **figura 3.4**.

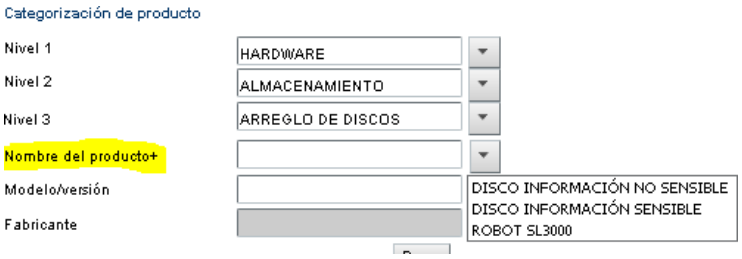


FIGURA 3.4 INFORMACIÓN SENSIBLE EN TICKET

Fuente: Autor

- **Respaldo de información**
  - Análisis causa raíz.

Problemática: No se ha realizado restauración de los respaldos en equipos del backbone

1. **¿Por qué no se ha realizado la restauración de los respaldos en los equipos del backbone?**: El proceso de restauración de un respaldo involucra un reinicio del equipo lo cual es un riesgo para el servicio.

2. **¿Por qué existe riesgo en el reinicio de los equipos?**: Por la cantidad de tráfico que cursa por estos equipos ya que son los dispositivos centrales de la red.

3. **¿Por qué importa tanto el tráfico que cursa por los equipos del backbone?** Si durante el apagado del equipo existiera un segundo evento (corte de fibra, daño en otro equipo) se verían afectados muchos de los servicios críticos de la empresa.

4. **¿Por qué podría afectar el presentar un segundo evento que afecte el backbone?** El backbone está formado por 4 equipos, uno en cada central, por lo que al apagar un equipo el anillo, pasaría a ser solo de 3. Si se presenta un segundo evento, una de las centrales podría perder conexión y los servicios que cursan por la misma se afectarían.

5. **¿Por qué no se tiene redundancia en cada central para los equipos del backbone?** Debido a la robustez de los equipos y costo de estos no amerita colocar 2 equipos redundantes por central, lo que si se tiene son redundancia a nivel de enlaces con los otros 3 equipos centrales.

- **Plan de acción**: Se elabora junto con el proveedor de los enrutadores un procedimiento para realizar la restauración de los respaldos obtenidos en el PHOENIX para realizarlo de forma anual durante una ventana de mantenimiento coordinada.

- **Resultado**: Luego de 15 días en revisiones con el proveedor y coordinación del trabajo, se realiza la restauración sobre uno de los equipos del backbone. El procedimiento consiste en descargar el respaldo del sistema PHOENIX, mediante un aplicativo llamado WINSCP se envía el respaldo al enrutador. Se especifica al enrutador que en su siguiente arranque tome la configuración cargada del respaldo y se realiza un reinicio del enrutador. Se aplica el procedimiento de forma exitosa y se presenta las evidencias al auditor. En la **figura 3.5** se puede observar el respaldo cargado en el enrutador.

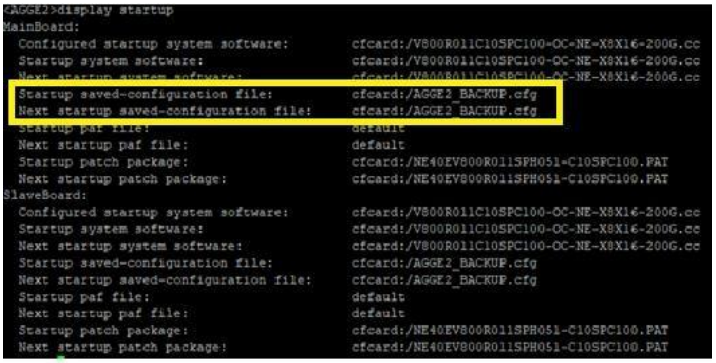


FIGURA 3.5 CARGA DE RESPALDO EN ENRUTADOR

Fuente: Autor

Una vez que todas las áreas que obtuvieron no conformidades en alguno de sus controles presentaron su plan de acción y que se sustentó las evidencias sobre la corrección de la no conformidad mayor, la entidad de certificación notificó a la compañía que ha obtenido la certificación bajo la norma ISO27001:2013 para el proceso de monitoreo del backbone de datos y servicios cloud. Las no conformidades menores se fueron resolviendo y presentando evidencias en el transcurso de los siguientes 45 días.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

La empresa ha logrado obtener la certificación del proceso de monitoreo del backbone de datos y servicios cloud bajo la norma ISO27001:2013 y este proyecto nos ha permitido obtener las siguientes conclusiones.

1. Las áreas de marketing y ventas se encuentran trabajando arduamente para aprovechar la certificación obtenida para la captación de clientes. Desde el área de transporte de datos si se ha notado un incremento de las configuraciones solicitadas para transporte de clientes en la nube en al menos un 25% de solicitudes luego de 6 meses de haber obtenido la certificación.

2. La identificación correcta de los activos de la información es la base para poder obtener una certificación, uno de los puntos que causó mayor complicación durante la auditoría externa fue la falla del sistema de documentación de procesos que fue evaluado con un nivel de riesgo bajo cuando en realidad si se debe especificar como crítico para la compañía y se deben tomar acciones para contar con redundancias en caso de fallos.

3. Pese a que la compañía por su antigüedad, experiencia y cumplimiento de otras normas ha ido documentando sus procesos y procedimientos, fue arduo el trabajo de realizar una homologación de los manuales existentes con los controles requeridos por la ISO 27001. El trabajo conjunto de las diversas áreas involucradas fue clave para poder encontrar los controles adecuados.

4. Las acciones tanto preventiva como correctivas que se han implementado como parte del proyecto de certificación han servido también para otros activos que no son parte del alcance del SGSI. Se ha logrado incrementar en el personal el interés sobre la seguridad de la información.

5. El área de auditoría pudo obtener experiencia en la norma ISO27001, por lo que la empresa está mejor preparada para las siguientes etapas que consisten en mantener la certificación. Los procesos han quedado claramente documentados para evitar que la rotación de personal cause inconvenientes en la recertificación y las auditorías de seguimiento.

RECOMENDACIONES

1. El personal involucrado por parte de cada área en el proyecto de certificación fue reducido, de 1 a 2 personas por jefatura, para evitar retrasos en las demás actividades operativas. Para las auditorías de seguimiento y el próximo proceso de recertificación, se debe involucrar personal distinto para extender el número de personas que conocen de los controles involucrados.

2. Se requiere que la alta dirección y presidencia siga comprometida con las mejoras sobre el SGSI, que no se tome esto como un proceso netamente comercial, sino que permite asegurar los activos de la compañía. De ser posible asignar recursos para que se puedan certificar otros procesos críticos para la compañía como es el segmento móvil masivo.

3. En la compañía cuando ingresa un nuevo empleado se realizan algunos cursos para que se obtenga conocimiento de la compañía, se sugiere colocar un curso destinado a la seguridad de la información y a la certificación obtenida para que se tenga un contexto de la importancia de esta.

BIBLIOGRAFÍA

[1] **EKOS**, Ataques informáticos a empresas públicas crecen 56% en el mundo https://www.ekosnegocios.com/articulo/ataques-informaticos-a-empresas-publicas-crecen-56-en-el-mundo, 2021.

[2] **ISO27001.ES**, Certificación ISO/IEC 27001 https://www.iso27000.es/certificacion.html, 2005.

[3] **López – Aguirre – Romero**, Introducción a los fundamentos de la seguridad informática http://reader.digitalbooks.pro/content/preview/books/102400/book/OEBPS/ch_2.html, 2006.

[4] **Juan Martín**, Estudia tu entorno con un PEST-EL https://www.cerem.ec/blog/estudia-tu-entorno-con-un-pest-el, 2017.

[5] **Enredando Proyectos**, La gestión de los riesgos en los proyectos https://enredandoproyectos.com/la-gestion-de-los-riesgos-en-los-proyectos/, 2019.

ANEXO A

ACTIVOS DE INFORMACIÓN DEL ÁREA DE O&M

Fuente: Autor

ID	NOMBRE	CAPA	TIPO	DESCRIPCIÓN	DUEÑO	CUSTODIO	UBICACIÓN
A001	CENTRAL GYE NORTE	ENTORNO	INSTALACIONES	LUGAR DONDE ESTÁN LOS EQUIPOS DE RED	GERENTE DE O&M	JEFE DE DATACENTER GYE	GYE NORTE
A002	CENTRAL GYE SUR						GYE SUR
A003	CENTRAL UIO NORTE					JEFE DE DATACENTER UIO	UIO NORTE
A004	CENTRAL UIO SUR						UIO SUR
A005	OFICINAS GYE NORTE	ENTORNO	INSTALACIONES	OFICINA DONDE ESTÁ PERSONAL DE O&M	GERENTE DE O&M	JEFE DE TRANSPORTE DATOS	GYE NORTE
A006	OFICINAS UIO NORTE						UIO NORTE
A007	INGENIEROS NOC	ENTORNO	PERSONAL	PERSONAL DEL NOC, MONITOREO	GERENTE DE O&M	JEFE DE NOC	GYE NORTE
A008	INGENIEROS TRANSPORTE DATOS GYE	ENTORNO	PERSONAL	PERSONAL DE O&M TRANSPORTE DATOS	GERENTE DE O&M	JEFE DE TRANSPORTE DATOS	GYE NORTE
A009	INGENIEROS TRANSPORTE DATOS UIO	ENTORNO	PERSONAL	PERSONAL DE O&M TRANSPORTE DATOS	GERENTE DE O&M	JEFE DE TRANSPORTE DATOS	UIO NORTE
A010	INGENIEROS DATACENTER GYE	ENTORNO	PERSONAL	PERSONAL DE O&M DATACENTER	GERENTE DE O&M	JEFE DE DATACENTER GYE	GYE NORTE

A011	INGENIEROS DATACENTER UIO	ENTORNO	PERSONAL	PERSONAL DE O&M DATACENTER	GERENTE DE O&M	JEFE DE DATACENTER UIO	UIO NORTE
A012	P_GYE_NOR	ENTORNO	EQUIPOS Y SUMINISTRO	ENRUTADOR DISPOSITIVO FÍSICO	GERENTE DE O&M	JEFE DE DATACENTER GYE	GYE NORTE
A013	P_GYE_SUR						GYE SUR
A014	P_UIO_NOR					JEFE DE DATACENTER UIO	UIO NORTE
A015	P_UIO_SUR						UIO SUR
A016	P_GYE_NOR	EQUIPOS DE COMPUTO	SISTEMA OPERATIVO	SOFTWARE DEL ENRUTADOR	GERENTE DE O&M	JEFE DE TRANSPORTE DATOS	GYE NORTE
A017	P_GYE_SUR						GYE SUR
A018	P_UIO_NOR						UIO NORTE
A019	P_UIO_SUR						UIO SUR

ANEXO B

RIESGOS ASOCIADOS A LOS ACTIVOS DE LA INFORMACIÓN

Fuente Autor

ID ACTIVO	ID RIESGO	AMENAZA	VULNERABILIDAD	PROBABILIDAD	IMPACTO	NIVEL DE RIESGO
A001, A002, A003, A004	GA1R01	Acceso físico no autorizado	Ausencia de control de acceso o fallas de este	Baja	Muy alto	Muy alto
	GA1R02	Robo o daños ocasionado por personal externo	Ausencia de control de acceso o fallas de este	Baja	Muy alto	Muy alto
	GA1R03	Daños de equipo por problemas de suministro	Falta de medidas de protección o monitoreo inadecuado de las medidas	Baja	Muy alto	Muy alto
	GA1R04	Daños de equipo por problemas de suministro	Deficiencia de mantenimientos de equipos e instalaciones	Baja	Muy alto	Muy alto
A005, A006	GA2R01	Acceso físico no autorizado	Ausencia de control de acceso o fallas del mismo	Muy baja	Muy alto	Alto
	GA2R02	Robo o daños ocasionado por personal externo	Ausencia de control de acceso o fallas del mismo	Muy baja	Muy alto	Alto
	GA2R03	Daños de equipo por problemas de suministro	Falta de medidas de protección o monitoreo inadecuado de las medidas	Muy baja	Muy alto	Alto
	GA2R04	Daños de equipo por problemas de suministro	Deficiencia de mantenimientos de equipos e instalaciones	Muy baja	Muy alto	Alto
A007, A008, A009,	GA3R01	Acceso o cambios en equipos no autorizados	Segregación de funciones del personal deficiente	Muy alta	Muy alto	Muy alto

A010, A011	GA3R02	Divulgación de información	Desconocimiento de normativas de seguridad y acuerdos de confidencialidad	Alta	Muy alto	Muy alto
	GA3R03	Errores de usuarios	Falta de instructivos operacionales sobre actividades	Alta	Muy alto	Muy alto
	GA3R04	Errores de usuarios	Ausencia de esquema de reemplazos	Media	Muy alto	Muy alto
A012, A013, A014, A015	GA4R01	Daño en el dispositivo o datos del mismo	Falta de mantenimiento de los equipos	Baja	Muy alto	Muy alto
	GA4R02	Deterioro en los servicios prestados por terceros	SLAs no definidos con proveedores o no monitoreados	Alta	Muy alto	Muy alto
A016, A017, A018, A019	GA5R01	Acceso o modificación no autorizada de los datos	Falta de un sistema de autenticación fuerte	Alta	Muy alto	Muy alto
	GA5R02	Acceso o modificación no autorizada de los datos	Mal manejo de las cuentas privilegiadas	Media	Muy alto	Muy alto
	GA5R03	Acceso o modificación no autorizada de los datos	Falta de auditoría de los logs de actividades sobre los equipos	Alta	Muy alto	Muy alto
	GA5R04	Daño de datos y equipo	Ausencia de procedimientos de detección de vulnerabilidades	Muy baja	Muy alto	Muy alto

ANEXO C

CONTROLES APLICADOS SOBRE LOS RIESGOS

Fuente: Autor

ID RIESGO	ID CONTROL	ANEXO A	DESCRIPCIÓN	DETALLE DE CONTROL	SOPORTE	RIESGO RESIDUAL
GA1R01	GA1R01C01	A.11.1.2	Controles físicos de entrada	Las solicitudes de ingreso a las centrales son aprobadas por jefatura de datacenter mediante un portal de acceso.	Manual TI-007. Solicitudes en portal.	Bajo
	GA1R01C02	A.11.1.1	Perímetro de seguridad física	Existe personal de seguridad en las centrales durante las 24 horas.	Manual SF-024.	
GA1R02	GA1R02C01	A.11.1.2	Controles físicos de entrada	Se lleva control de los materiales con que ingresa el personal y se revisan los mismos al salir de la central.	Manual TI-007. Solicitudes en portal.	Medio
GA1R03	GA1R03C01	A.11.2.1	Emplazamiento y protección de equipos	Para cada nuevo equipo se realizan pruebas de aceptación donde se valida cumplimiento de normas eléctricas.	Acta de aceptación de nuevo equipo.	Bajo
	GA1R03C02	A.11.2.2	Instalaciones de suministro	Mantenimiento preventivo mensual de los sistemas	Manual TI-076	

				de respaldo eléctrico.		
	GA1R03C03	A.11.2.3	Seguridad del cableado	Para cada nuevo equipo se realizan pruebas de aceptación donde se valida cumplimiento de normas de cableado estructurado.	Acta de aceptación de nuevo equipo.	
GA1R04	GA1R04C01	A.11.2.4	Mantenimiento de los equipos	Mantenimiento preventivo acorde a cronograma de planificación.	Manual TI-076	Bajo
GA2R01	GA2R01C01	A.9.1.1	Política de control de acceso	La empresa cuenta con políticas claras para la seguridad física y control de acceso.	Manual SF-024.	Bajo
	GA2R01C02	A.11.1.2	Controles físicos de entrada	Se cuenta con procedimientos definidos para el ingreso de personal y terceros.	Manual SF-024.	
GA2R02	GA2R02C01	A.9.1.1	Política de control de acceso	La empresa cuenta con políticas claras para la seguridad física y control de acceso.	Manual SF-024.	Bajo
	GA2R02C02	A.11.1.2	Controles físicos de entrada	Se cuenta con procedimientos definidos para el ingreso de	Manual SF-024.	

				personal y terceros.		
GA2R03	GA2R03C01	A.11.2.2	Instalaciones de suministro	Mantenimiento preventivo mensual de los sistemas de respaldo eléctrico.	Manual TI-076	Bajo
GA2R04	GA2R04C01	A.11.2.4	Mantenimiento de los equipos	Mantenimiento preventivo acorde a cronograma de planificación.	Manual TI-076	Bajo
	GA2R04C02	A.17.1.2	Implementar continuidad de seguridad de la información	Simulacros del plan de contingencia, permiten identificar el estado de los sistemas.	Manual plan de contingencia	
GA3R01	GA3R01C01	A.6.1.2	Segregación de tareas	Se tiene definida la matriz de roles vs cargos que detalla perfil de cada usuario.	Manual TI-058	Bajo
	GA3R01C02	A.9.1.1	Política de control de acceso	Existe un proceso de registro, verificación y aprobación de los accesos de los usuarios.	Manual TI-091	
GA3R02	GA3R02C01	A.7.1.2	Términos y condiciones del empleo	En el proceso de contratación se incluye documento de “Declaración de confiabilidad” .	Documento “Declaración de confiabilidad”	Bajo

	GA3R02C02	A.7.2.2	Concienciación, educación y capacitación en seguridad de la información	La empresa cuenta con programas de concienciación a los que son sus inscritos sus empleados.	Correos de TH incluyendo a personal en programas de seguridad	
GA3R03	GA3R03C01	A.12.1.1	Documentación de procedimientos operacionales	Los procedimientos operacionales se encuentran definidos para la gerencia de O&M	Manual TI-014	Bajo
GA3R04	GA3R04C01	A.6.1.1	Roles y responsabilidades en la seguridad de la información	Los roles de los ingenieros están definidos en políticas.	Manual TI-058	Bajo
	GA3R04C02	A.7.3.1	Responsabilidades ante finalización o cambio	Las responsabilidades en caso de cambio o finalización están definidas en el código de ética.	Código de ética presente en la intranet	
GA4R01	GA4R01C01	A.11.2.4	Mantenimiento de los equipos	Mantenimiento preventivo acorde a cronograma de planificación.	Manual TI-076	Medio
GA4R02	GA4R02C01	A.15.2.1	Control y revisión de la provisión de servicios del proveedor	Se realiza supervisión de los trabajos de mantenimientos realizados por el proveedor.	Manual TI-076	Bajo

	GA4R02C02	A.15.2.2	Gestión de cambios en la provisión del servicio del proveedor	Se registra bitácora de cambios en la programación y ejecución de mantenimientos.	Manual TI-076	
GA5R01	GA5R01C01	A.9.1.1	Política de control de acceso	Se tiene control de acceso lógico a los equipos mediante una autenticación central con servidor TACACS.	Manual TI-091	Bajo
	GA5R01C02	A.9.2.1	Registro y baja de usuario	Existe procedimientos para creación, eliminación y cambios de usuarios definidos mediante portal web.	Manual TI-091	
GA5R02	GA5R02C01	A.9.2.2	Provisión de acceso de usuario	La creación de usuarios se realiza desde el portal web llamado SST.	Manual TI-091	Bajo
	GA5R02C02	A.9.2.3	Gestión de privilegios de acceso	Los privilegios de los usuarios solo cambian si son autorizados por Gerencias y jefaturas involucradas.	Manual TI-091	
	GA5R02C03	A.9.2.6	Retirada o reasignación de los derechos de acceso	En caso de cambios o retiros de personal existen procedimientos para la	Manual TI-091	

				regularización del usuario.		
GA5R03	GA5R03C01	A.12.4.3	Registros de administración y operación	Los logs de las actividades de los usuarios son almacenados dentro del servidor TACACs	Manual TI-091	Bajo
	GA5R03C02	A.13.1.1	Controles de red	Los permisos de red hacia los elementos pasan por un proceso de aprobación mediante el portal SST.	Manual TI-072	
GA5R04	GA5R04C01	A.12.6.1	Gestión de las vulnerabilidades técnicas	Análisis de vulnerabilidades realizado de forma anual por el proveedor.	Manual SL-008	Medio

ANEXO D

PLAN DE TRATAMIENTO

Fuente: Autor

ID RIESGO	RIESGO RESIDUAL	OPCIÓN DE TRATAMIENTO	PLAN DE ACCIÓN
GA1R01	Bajo	Mitigar	El portal actual solo permite ingreso de nombres de personal que ingresará a la central, se implementará un nuevo portal donde los usuarios subirán fotos de las cédulas del personal que ingresará.
GA1R02	Medio	Mitigar	Cambios en el manual TI-007, donde se incluirá que el personal externo solo puede ingresar acompañado por personal de la empresa; salvo casos emergentes aprobados por la jefatura de datacenter.
GA1R03	Bajo	Transferir	Solicitar al proveedor actualización de las normas de respaldos tanto eléctricos como de climatización que permitan mantener el centro de datos operativo. Ajustar las penalidades con el proveedor en casos de fallas del sistema redundante.
GA1R04	Bajo	Asumir	Se posee un sistema y procedimientos de fiscalización de los mantenimientos realizados por los proveedores que permite tener control y realizar los ajustes. No se observa oportunidad de mejora.
GA2R01	Bajo	Mitigar	Cambios en la forma en que se lleva la bitácora de ingreso a oficinas, actualmente el control se lleva por correo a consola de seguridad. Se realizará integración al portal de ingreso a centrales para que la bitácora quede en un sistema de información y no en un libro físico ubicado en la garita.

GA2R02	Bajo	Mitigar	Personal de seguridad debe tomar fotos de los elementos con que ingresa el personal a las oficinas y de igual forma al salir de las mismas. Estas quedarán registradas en el portal.
GA2R03	Bajo	Transferir	Solicitar al proveedor actualización de las normas de respaldos tanto eléctricos como de climatización que permitan mantener el centro de datos operativo. Ajustar las penalidades con el proveedor en casos de fallas del sistema redundante.
GA2R04	Bajo	Asumir	Se posee un sistema y procedimientos de fiscalización de los mantenimientos realizados por los proveedores que permite tener control y realizar los ajustes. No se observa oportunidad de mejora.
GA3R01	Bajo	Mitigar	Revisar los roles definidos en el manual existente ya que han existido fusiones de áreas y creación de nuevas áreas en la empresa. Actualizar el manual en base a las revisiones realizadas.
GA3R02	Bajo	Mitigar	La gerencia de O&M se compromete a enviar recordatorios semestrales sobre la realización de cursos relacionados al código de ética y recordar los puntos clave del mismo para que su personal pueda cumplirlo.
GA3R03	Bajo	Mitigar	Realizar la revisión de los instructivos operacionales existentes definidos en el manual TI-014. Para el área de transporte de datos se definirá el instructivo ya que no existe actualmente.
GA3R04	Bajo	Mitigar	La gerencia de O&M se compromete a enviar recordatorios semestrales sobre la realización de cursos relacionados al código de ética y recordar los puntos clave de este para que su personal pueda cumplirlo.
GA4R01	Medio	Transferir	Solicitar al proveedor actualización de las normas de respaldos tanto eléctricos como de climatización que permitan mantener el centro de datos operativo. Ajustar las

			penalidades con el proveedor en casos de fallas del sistema redundante.
GA4R02	Bajo	Asumir	Los niveles de SLA con el proveedor se encuentran claros, reducir los tiempos de atención o solicitar incremento del personal del proveedor requeriría un presupuesto adicional del que no se cuenta.
GA5R01	Bajo	Mitigar	Realizar una revisión semestral de los usuarios que se tienen creados y depurar aquellos que ya no requieren acceso.
GA5R02	Bajo	Mitigar	Realizar una revisión semestral de las cuentas con niveles privilegiados sobre los equipos, esto solo debe ser constante para el personal de transporte datos.
GA5R03	Bajo	Mitigar	Mantener control sobre la cantidad de solicitudes de acceso a elementos de red de forma mensual. Revisar los logs en casos emergentes.
GA5R04	Medio	Transferir	Contratar una empresa especializada para realizar un análisis de las vulnerabilidades que se puedan encontrar en los dispositivos.