Historia

DOCUMENTO SOBRE EL ALCANCE DEL SGSI

HISTORIA

Versión	Fecha	Cambios Introducidos
1.0.0	**24/10/2022**	**Versión Inicial del Documento.**

TABLA DE CONTENIDOS

1. OBJETO, ALCANCE Y USUARIOS.

El objeto de este documento es definir cuales serán los limites para llevar a cabo el diseño del SGSI (sistema de gestión de seguridad de la información), para la empresa OBSS INGENIERÍA. También tiene los lineamientos de como los activos de información serán clasificados para su protección ante riesgos u/o amenazas.

Los usuarios de este documento corresponden a miembros de la dirección de redes y seguridad de la información de OBSS INGENIERÍA.

2. DOCUMENTO DE REFERENCIA

- Norma ISO/IEC: 27001:2003
- Documentos de cumplimiento mínimo para el diseño de la norma ISO 27001 para OBSS INGENIERÍA.
- Requisitos tanto normativos, contractuales y cualquier índole que permita asegurar el correcto diseño de la norma ISO 27001:2013 para OBSS INGENIERÍA.

3. REVISIÓN Y ACTUALIZACIÓN

El documento ALCANCE DEL SGSI, será revisado periódicamente y podrá estar sujeto a cualquier cambio u/o actualización que tendrá lugar en las oficinas de OBSS INGENIERÍA. En el momento en que se registre cualquier cambio que represente un valor agregado o sea muy significativo; el comité de seguridad de la información designado por OBSS INGENIERÍA tendrá que aplicar dicha actualización o modificación por un oficial de seguridad de la información y posteriormente deberá ser aprobado por el comité de seguridad de la información indicando las partes interesadas (empleados, proveedores, usuarios finales, clientes, contratistas etc).[1]

Revisión y Actualización.	Oficial de Seguridad de la Empresa OBSS INGENIERÍA
Aprobación	Comité de Seguridad de la información de OBSS INGENIERÍA
Adopción	(empleados, proveedores, usuarios finales, clientes, contratistas etc)

Tabla 1 Revisión y Actualización de Alcance de SGSI.

[1] https://www.notariasegunda.com/wp-content/uploads/2022/02/D.-NOT-SGSI-DSA01-Documento-sobre-el-alcance-del-SGSI-1.pdf

4. DEFINICIÓN DEL ALCANCE DE SGSI.

La empresa OBSS INGENIERÍA tiene como objeto que se lleve a cabo el diseño del SGSI basado en la norma ISO 27001, para ello es importante realizar la definición de cuales serán los límites dicho diseño, esto con el objetivo de decidir cual será la información que se quiere proteger. Cuando se lleve a cabo la clasificación de los activos, se indicará que esa información deberá protegida sin importar si es almacenada, procesada, transmitida o transferida dentro o fuera de las instalaciones de OBSS INGENIERÍA.

Si alguna información llega a estar fuera del alcance no implica que no se le daban aplicar las respectivas normas o medidas de seguridad; esto solo se verá como la responsabilidad de que esta seguridad sea ser transferida a un tercero que pueda llegar alterar y vulnerar dicha información, por ello es importante recordar que la seguridad de la información es para proteger todos los activos de información o cualquier dato que pueda involucrar el desempeño normal o exitoso de sus funciones, servicios o cualquier actividad de OBSS INGENIERÍA.

Dentro de los activos que se protegen son ubicaciones físicas, información impresa, electrónica, registros y cualquier procedimiento como software o licencias entre otros.

Tomando en cuenta los requisitos legales, normativos, contractuales y de otra índole, el alcance del SGSI se define de acuerdo con los siguientes aspectos

4.1 PROCESOS Y SERVICIOS.

El proceso de seguridad de la información tiene aplicabilidad a cualquier función, servicio, actividad y activos de información del proceso de suministro de servicios de Conectividad por medio de Radio Enlace para usuarios finales, que se identifica como parte de la cadena de valor establecido por OBSS INGENIERÍA.

Dirección de Redes.

Gerente General:

La dirección de Redes es la encargada de llevar todo el control de los proyectos, estructurar los comités y realizar la evaluación y sustentación de proyectos de gran escala. Las actividades corresponden a:

- Procurar la disponibilidad de recursos para la implementación de proyectos: Valida que efectivamente se cuenten con todos los recursos para llevar a cabo una excelente implementación de los proyectos, validando los riesgos del proyecto.
- Monitorear que se esté cumpliendo los indicadores financieros de la empresa: Revisar periódicamente que se cumple con la meta financiera de la dirección de redes y así mismo solicitar a la gerencia general la aprobación de capex para llevar a cabo implementaciones de los activos.
- Vigilar que los requisitos del cliente se determinen y se cumplan: Revisar juntamente con los ingenieros y técnicos que los requisitos del cliente cumplan los más altos estándares de ingeniería para su correcto funcionamiento.

Líder Técnico: asigna los proyectos al comercial y da el aval de las solicitudes comerciales para llevar a cabo el respectivo acompañamiento de este.

A continuación, parte de las actividades que apoyará:

- Acompañar y apoyar por el cumplimiento del SGSI.
- Lograr certificaciones para equipo de trabajo técnico de la empresa.
- Proporcionar apoyo de diseño de ingeniería para los proyectos nuevos.
- Fijar los objetivos de su equipo de trabajo.

Arquitecto de Redes: Recibe los proyectos asignados por el líder técnico y realizará toda la comprensión y arquitectura para lograr una ejecución efectiva de ingeniería para proveer el servicio requerido por el cliente o los usuarios finales.

A continuación, se detalla las actividades o responsabilidades:

- Entender en detalle los requerimientos del cliente.
- Diseñar, preparar y sustentar los diseños del proyecto.
- Documentar los casos de éxitos de implementación de proyectos.
- Realizar Cotización con los fabricantes o proveedores de la infraestructura adquirir para los proyectos.
- Apoyar en la implementación de los proyectos de ingeniería.
- Gestionar a los equipos involucrados.

Técnico de Redes: El técnico de redes se encarga de llevar a cabo las visitas, instalar, verificar, realizar mantenimiento preventivos y correctivos, configuraciones y brindar el soporte a cliente final ante fallas de los servicios adquiridos por los clientes.

- A continuación, las responsabilidades:
- Asistir a los programas de Entrenamientos y capacitación suministrado por la empresa OBSS.
- Participar activamente en los Comités internos de mejora de los procesos de OBSS.
- Ejecutar los proyectos definidos, cumpliendo con el alcance definido por el área de Redes de OBSS, diseño de Arquitectura.
- Administrar la implementación, funcionamiento, actualización y mantenimiento preventivo y correctivo de la infraestructura de cada uno de los NODOS de la empresa OBSS.
- Realizar Diagnostico de las necesidades de hardware y software para la empresa OBSS.
- Documentar correctamente las instalaciones realizadas.
- Asegurar la entrega del servicio en nivel de satisfacción alto.

4.2 UNIDADES ORGANIZATIVAS.

La estructura organizaciones de la seguridad de la información de OBSS INGENIERÍA es un esquema que se define y se aprueba, donde se identifican todas las dependencias que son funcionales y estratégicas para la protección de la seguridad de la información para OBSS INGENIERÍA.

OBSS INGENIERÍA tiene actualmente un grupo laboral de 10 -15 empleados que diariamente están procesando información y para poder lograr que los servicios o actividades mencionadas anteriormente se cumplan se debe fortalecer en la medida esta fuerza laboral.

Como se menciono anteriormente las actividades de OBSS INGENIERÍA, la hace responsable de prestar un servicio de calidad como es el aprovisionamiento de Internet por medio de canales de radio enlace.

Las unidades organizativas que se encuentran delimitadas dentro del alcance del SGSI en OBSS INGENIERÍA son:

Dirección	Cargo	Autoridad
Dirección de Redes	Gerente General	Aprobar los documentos y planes para SGSI. Aprobación y adopción del SGSI. Asegurar que se realicen las acciones (preventivas, Correctivas, Mejora) cuando sea necesario. Aprobar documentos financieros e indicadores financieros de la empresa. Aprobar proyectos de alto impacto.
Responsable Técnico	Líder Técnico	Aprobar la oferta técnico-económica para presentar a cliente final. Aprobar los Flujos de implementación de las etapas contractuales. Asegurar que se implemente el SGSI acorde a necesidad. Aprobar los informes y pruebas realizadas en la implementación de proyecto. Asegurar que se lleven a cabo los comités de inicio de proyecto.

Dirección de Redes	Arquitecto de Redes	Asignar actividades de diseño a los técnicos de redes. Aprobar los diseños técnicos de diseño. Aprobar los flujos de trabajo junto con el Líder Técnico. Asegurar negociaciones con fabricantes o Terceros.
Dirección de Redes	Técnico de Redes	Asegurar los activos lleguen a los destinos de instalación de proyecto. Asegurar las certificaciones técnicas de fabricantes. Asegurar cumplimiento de cronograma con equipos de cuadrillas asociadas a proyecto. Apoyar en los comités internos de ingeniería. Aprobar el recibido de la infraestructura contratada. Aprobar los documentos de inventarios de infraestructura.

Dirección de Seguridad.	Oficial de Seguridad	Aprobar la documentación requerida para el diseño y posterior implementación del SGSI para OBSS. Aprobar el plan de adopción y capacitación del SGSI. Aprobar las características técnicas de los activos que adquiera OBSS a nivel de Seguridad. Asegurar personal de apoyo para la adopción del SGSI. Asegurar con los proveedores las capacitaciones de cultura del SGSI para OBSS. Mantener la seguridad y la confidencialidad sobre la emisión y mantenimiento de la identificación de usuarios y contraseñas Guiar al cuerpo directivo y a la administración de la organización ante incidentes de seguridad mediante un Plan de Respuesta a Incidentes, con el fin de atender rápidamente este tipo de eventualidades.

Dirección de Seguridad.	Profesional de Seguridad.	Asegurar los indicadores permanentes de seguridad de la información de OBSS. Solicitar al Oficial de Seguridad el acompañamiento en las recomendaciones de ciberseguridad, capacitación o concientización al interior de OBSS. Revisar con el Oficial de seguridad el cronograma de implementación de la SGSI. Identificar los riesgos de los activos de seguridad de OBSS. Disponer de la información para asegurar el SGSI. Aprobar las solicitudes de los usuarios para los accesos de información de la empresa OBSS. Definir e implementar políticas de seguridad acorde a las necesidades del cliente en cada proyecto en entornos de sistemas complejos y multi fabricante
Dirección de TI	Técnico de soporte	Identificar los requerimientos de los usuarios respecto a las instalaciones de software. Autorizar la creación de nuevas cuentas bajo el dominio de la empresa OBSS. Solicitar a los fabricantes las garantías de los equipos. Mantener al día los documentos de recibido a satisfacción de los usuarios. Fomentar estrategias del buen alistamiento de los equipos cumpliendo con la norma SGSI.

Dirección Comercial	Ejecutivo Comercial Senior.	Asginar la oportunidad al arquitecto de Redes. Identificar las necesidades del cliente y solicitar que se cumpla con lo requerido. Aprobar la oferta técnico-económica desde el área comercial. Asegurar los ingresos de OBSS.
Dirección Financiera	Contador.	Aprobar el capex requerido por la unidad de Redes de OBSS. Asegurar el cumplimiento de los trámites contables y tributarios requeridos normativamente, así como las respuestas requeridas por las autoridades y organismos de control.
Dirección de RRHH	Bussines Parner	Hay que asegurar que los empleados cumplan con los manuales de la empresa OBSS. Promover el buen uso de las herramientas de la compañía. Aprobar encuestas de clima de la empresa OBSS. Asegurar la documentación de los empleados de OBSS. Apoyar la cultura Organizacional.

4.3 UBICACIONES.

OBSS INGENIERÍA, cuenta con una distribución de dos plantas, como oficina principal, en LA primera planta se encuentran el área de ingeniería, todo lo referente a lo operativo (Dirección de Redes, Dirección de Seguridad de la información, área comercial) y en la planta 2 se encuentran las áreas administrativas como (compras, RRHH, financiera).

4.4 REDES E INFRAESTRUCTURA TI.

A continuación, se detalla la infraestructura:

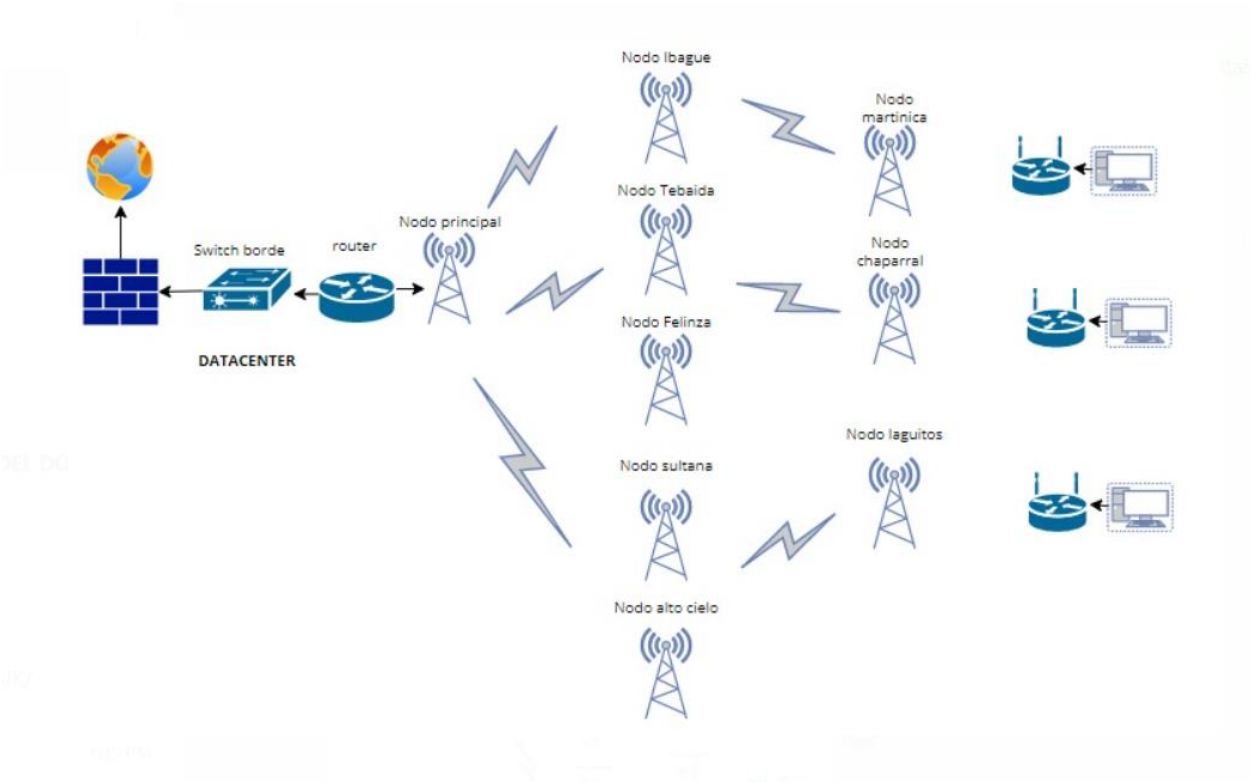
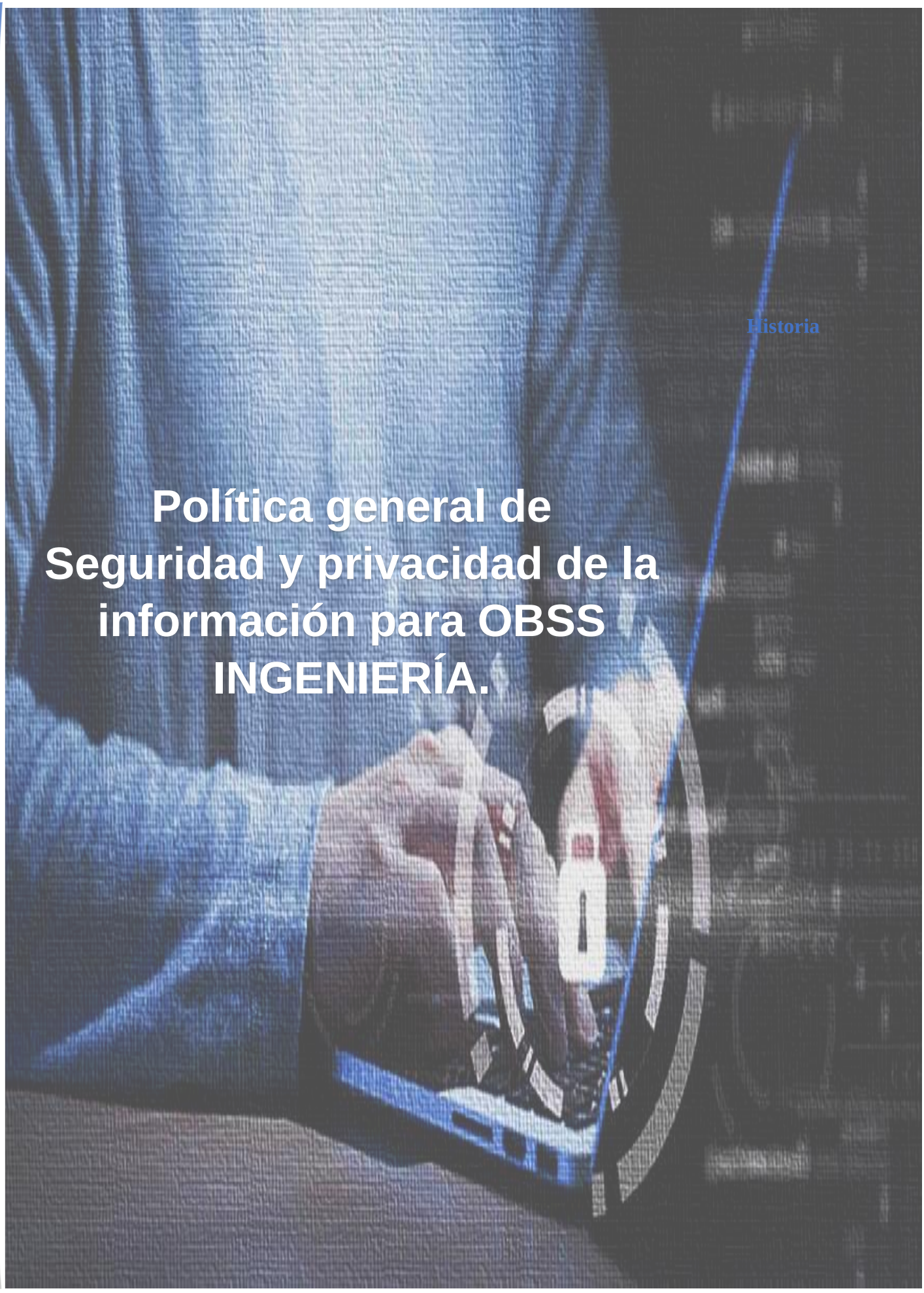


Ilustración 1 Diagrama Topológico de OBSS INGENIERÍA



Historia

Política general de Seguridad y privacidad de la información para OBSS INGENIERÍA.

HISTORIA

Versión	Fecha	Cambios Introducidos
1.0.0	**27/10/2022**	**Versión Inicial del Documento.**

TABLA DE CONTENIDOS

1. DERECHOS DE AUTOR.

2. AUDIENCIA

Este documento está elaborado para la empresa OBSS INGENIERÍA, y empresas del sector de telecomunicaciones a nivel regional, que requieran una guía para llevar a cabo el diseño e implementación del modelo de seguridad de la información, como también va dirigido a los proveedores de la empresa OBSS INGENIERÍA que deseen adoptar el modelo de seguridad y privacidad de la información.

3. INTRODUCCIÓN

La política general tiene como necesidad el diseño y posterior adopción de un sistema de gestión de seguridad de la información (SGSI), teniendo como planteamiento desde el diseño y descripción del porqué se debe diseñar e implementar un SGSI en una empresa como OBSS INGENIERÍA, cómo se debe llevar a cabo el diseño del SGSI y cuáles son los cumplimientos requeridos para lograr un buen diseño para luego realizar la respectiva implementación del SGSI.

Es así como se tiene en cuenta la importancia y necesidad de OBSS INGENIERÍA para su negocio tener definido e identificado las necesidades de las áreas y contar con una valoración previa de los controles para conservar la seguridad de la información, adicionalmente que es importante sentar una política del funcionamiento de la empresa, cuales son los objetivos de la empresa para el cumplimiento de la política en la prestación de sus servicios y que sea aprobada por la dirección de seguridad de OBSS INGENIERÍA.

Por tal razón es importante desarrollar una política concreta, de fácil cumplimiento y lectura sin excepción para aquellos que accedan a ella.

4. PROPÓSITO

Este formato puede ser utilizado como plantilla para que se pueda elaborar la política general de seguridad y privacidad de información para las empresas regionales y del sector de telecomunicaciones, que sean prestadoras de servicios de Internet para regiones tanto urbanas y rurales y que tienen como objetivo la prestación de servicios para clientes tanto del sector privado como público.

5. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

La dirección de OBSS INGENIERÍA, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para OBSS INGENIERÍA la protección de la información es fundamental y busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de esta, acorde con las necesidades de los diferentes grupos de interés identificados. De acuerdo con lo anterior, esta política aplica a OBSS INGENIERÍA según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.

- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de OBSS INGENIERÍA.
- Garantizar la continuidad del negocio frente a incidentes.

OBSS INGENIERÍA ha decidido junto con su equipo directivo apoyarse en en una consultoría para el diseño la definición y posterior implementación y operación de un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

Finalmente es de gran ayuda incluir la descripción general de otras políticas relevantes para el cumplimiento de los Objetivos planteados dentro del proyecto del SGSI ya que éstas son el apoyo sobre el cual se desarrolla; éstas deben ser descritas de forma sencilla, puntual y muy efectiva. Dentro de las temáticas que se tocan en este punto se encuentran por ejemplo la gestión de activos, seguridad física y ambiental, control de accesos, etc.

Para abordar este punto es necesario remitirse a la “Guía de políticas específicas de seguridad y privacidad de la información” y mencionar aquellas que OBSS INGENIERÍA haya establecido como necesarias y primordiales.

A continuación, se establecen 12 principios de seguridad que soportan el SGSI de OBSS INGENIERÍA:

- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, socios de negocio o terceros.
- OBSS INGENIERÍA protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.
- OBSS INGENIERÍA protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- OBSS INGENIERÍA protegerá su información de las amenazas originadas por parte del personal.
- OBSS INGENIERÍA protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- OBSS INGENIERÍA controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- OBSS INGENIERÍA implementará control de acceso a la información, sistemas y recursos de red.

- OBSS INGENIERÍA garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- OBSS INGENIERÍA garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- OBSS INGENIERÍA garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- OBSS INGENIERÍA garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

6. ALCANCE / APLICABILIDAD

Esta política aplica a toda la empresa OBSS INGENIERÍA, sus funcionarios, contratistas y terceros y la ciudadanía en general.

7. NIVEL DE CUMPLIMIENTO

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política.

8. FASES DE IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN.

Se recomienda a OBSS INGENIERÍA, posterior al diseño del plan de SGSI, realizar una correcta implementación de políticas de seguridad de la información, para ello es muy importante cumplir con las fases que se citarán a continuación, estás fases tienen como objetivo que OBSS INGENIERÍA desarrolle y socialice las políticas para un buen uso de todos los empleados, contratistas o terceros.

A continuación, las fases:

8.1 IMPORTANCIA DE LAS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN.

Las empresas sin importar su tamaño deben de contar con políticas de seguridad ya que, por medio de estas, se guiará el comportamiento personal y personal de los funcionarios, contratistas y proveedores terceros sobre la importancia de las mejores prácticas de seguridad y cumplir con los respectivos requisitos legales a los que se pueda ver obligada la empresa.

8.2 FASE DE IMPLEMENTACIÓN DE LAS POLITICAS DE SEGURIDAD DE INFORMACIÓN.

8.2.1 DESARROLLO DE POLÍTICAS

Esta fase tiene como objeto en responsabilizar a las áreas de la empresa para que se generen o creen las políticas de manera estructurada, bien escritas, luego pase a una etapa de revisión y aprobación; por lo que es muy importante llevar una muy buena investigación de verificación por lo que se deben seguir los siguientes aspectos:

- Justificación de la creación de política: Esta política permite que la empresa OBSS INGENIERÍA identifique por qué se requiere la creación de la política de seguridad de la información y que control se realizará para su diseño y posterior implementación.

- Alcance: Debe determinarse el alcance, ¿A qué población, áreas, procesos o departamentos aplica la política?, ¿Quién debe cumplir la política?

- Roles y Responsabilidades: Se debe definir los responsables y los roles para la implementación, aplicación, seguimiento y autorizaciones de la política.

- Revisión de la política: Es la actividad mediante la cual la política una vez haya sido redactada pasa a un procedimiento de evaluación por parte de otros individuos o grupo de individuos que evalúen la aplicabilidad, la redacción y se realizan sugerencias sobre el desarrollo y creación de esta.

• Aprobación de la Política: Se debe determinar al interior de la entidad la persona o rol de la alta dirección que tiene la competencia de formalizar las políticas de seguridad de la información mediante la firma y publicación de estas. Es importante que la Alta Gerencia de la Entidad muestre interés y apoyo en la implementación de dichas políticas.

8.2.2 CUMPLIMIENTO:

La fase de cumplimiento es aquella donde todas las políticas escritas o que se estipulan en el diseño del SGSI basado en la norma ISO 27001:2013, deben ser implementados y estar relacionados con los controles de seguridad de la información, ya que esto permitirá que exista una base solida entre los que se diseña versus los controles de seguridad ya implementados y posteriormente documentados.

8.2.3 COMUNICACIÓN:

La fase de Comunicación es la que permite conocer a los empleados de OBSS INGENIERÍA cuales son las políticas diseñadas y bajo que norma se han tenido en cuenta, es importante que al igual que los funcionarios o empleados de la empresa, los contratistas, proveedores y/o terceros de OBSS INGENIERÍA estén enterados de ellas. Esta fase es de las más importantes ya que cualquier conocimiento que se transmita a los empleados de OBSS INGENIERÍA, deberán quedar plasmado en las políticas y la aplicabilidad de estas dependerá del conocimiento de estas. Cuando OBSS INGENIERÍA inicie su fase de implementación permitirá realizar una retroalimentación de cuan efectivas son a partir del diseño, y se procederá a las respectivas correcciones para dar cumplimiento de estas.

8.2.4 MONITOREO

La fase de monitoreo es importante porque permitirá que OBSS INGENIERÍA determine que tan efectiva y que tanto cumplimiento de las políticas se ha realizado durante la etapa tanto de diseño como implementación del SGSI. Para ello es importante que la empresa cree mecanismos de indicadores para que sean verificadas de manera periódica y con evidencias si deben o no ajustarse.

8.2.5 MANTENIMIENTO

Esta fase asegura que las políticas diseñadas estén implementadas en su correcto orden, adicionalmente que se realice la respectiva actualización, integración y socialización, por lo que si de haber correcciones se tendrán que hacer los ajustes necesarios por medio de las retroalimentaciones obtenidas.

8.2.6 RETIRO

Esta fase es importante tenerla indicada en la política de seguridad y privacidad, porque cuando una política ha cumplido con su objetivo u finalidad se tendrá que evaluar que tan necesaria es seguir manteniéndola o si definitivamente se debe retirar de la política, por ello se considera como una ultima fase ya que cualquier política establecida debe quedar registrada o documentada con el objetivo de poder tener referencias o cualquier antecedente de esta.

9. POLÍTICAS DE SEGURIDAD IDENTIFICADAS PARA OBSS INGENIERÍA.

9.1 POLÍTICA DE SEGURIDAD FÍSICA Y DEL ENTORNO.

- **Acceso**

Para la política de seguridad física y del entorno, Se debe tener controlado y restringido los accesos a los cuartos de equipos principales de la organización, los cuartos de redes y todo lo que contenga activos, pues la empresa debe contar con un protocolo que solo permita el ingreso al personal que dispone de las credenciales y autorización para el respectivo ingreso.

- **Seguridad de los Equipos**

Todos los equipos de la compañía donde transite información o contenga información y servicios confidenciales deben estar alojados en ambientes seguros y protegidos para garantizar que no sea adulterada ningún tipo de información, o se tenga ingreso a los equipos y se pueda evidenciar un alto riesgo. Para ello es importante tener en cuenta:

• Que los controles de acceso y la seguridad física solo estén autorizadas al personal técnico y profesional de la compañía.

• Realizar el acompañamiento a estos cuartos cuando personas que no estén autorizadas como los proveedores de servicios o terceros lleguen a realizar cualquier tipo de mantenimiento preventivo y correctivos.

• Garantizar un monitoreo mediante sensores de movimientos y cámaras de seguridad.

• Disponer de todas las herramientas de seguridad industrial (Detectores de humo, iluminaria de emergencia, extintores, protocolos de seguridad para empleados) en caso de algún evento externo o ajeno a la operación como: incendios, terremotos, inundaciones etc.

Análisis de Riesgos

• La protección de los equipos debe ser garantizada con sistemas regulados como pararrayos, UPS y conexiones a tierra.

• Se debe garantizar la protección de los equipos para eventualidades de falla eléctrica con bancos de baterías para no presentar interrupciones en los servicios.

• Realizar mantenimientos preventivos y correctivos de los equipos core de la compañía para garantizar la disponibilidad.

• Garantizar que los equipos cuentes con respaldos a nivel de disponibilidad de los servicios, es decir contar con canales BACKUP y equipos de Backus si un servicio de canal de datos o internet falla ingrese el otro automáticamente.

- **Política de Control de Accesos**.

El acceso en seguridad de la información tiene como objeto a la identificación, autenticación y autorización de los usuarios que acceden a los sistemas, recursos o a las áreas de la compañía para ello se le han delegado los respectivos permisos necesarios para garantizar la disponibilidad, confidencialidad e integridad de la información de los activos ya sea a nivel de Software y/o hardware. (Supersubsidio, 2018) Se tiene identificado los siguientes controles de acceso para la compañía OBSS INGENIERÍA.

• Acceso Físico

• Acceso Lógico

- **Acceso Físico**

Las normas de seguridad para el control de Acceso Físico deben garantizar en la identificación del personal que va a tener acceso tanto a las instalaciones de la organización, como a los cuartos de equipos y centro de datos, esto con el fin de poder garantizar los respectivos privilegios de acceso físico, para ello es importante tener en cuenta los siguientes ítems:

• Se debe llevar un registro muy detallado de todos los visitantes que ingresen a las áreas protegidas.

• Se debe controlar y limitar el acceso a la información que es de carácter clasificada sobre los activos como los equipos enrutadores, servidores, Switches, Equipos WLAN e.t.c

• Todas las puertas de acceso a los cuartos donde se encuentre los equipos core de la compañía debe contar con controles de acceso biométricos, o lectores de tarjetas la cual limita y hace seguro el acceso a estos cuartos.

• Se debe manejar formatos donde quede por escrito las aprobaciones de las solicitudes de acceso de terceros, contratistas y personal de mantenimiento. Además, se debe realizar el respectivo acompañamiento en las áreas mencionadas.

• Las tarjetas de acceso o las autorizaciones que se les otorga a los terceros, contratistas o personal externo a la compañía deben ser limitado es decir solo se debe permitir el ingreso a puertas donde no se vulnere ningún activo de la compañía.

• Se debe garantizar que la devolución de carnet de acceso sea devuelta por la persona externa de la compañía.

• El personal de la compañía debe solicitar al área de seguridad de la compañía autorización por escrito cualquier acceso de persona externa de la compañía y cualquier daño, o violación de las normas internas será responsabilidad del empleado.

- **Acceso lógico.**

• Los líderes del área encargada deben ser el único que tenga todos los privilegios de acceso a los servicios de red, plataformas o a los sistemas de información.

• La administración de perfiles de usuario es responsabilidad de cada administrador de plataforma.

• Los administradores de las diferentes plataformas de la compañía será el responsable y contará con los privilegios y permisos para crear, modificar, bloquear o eliminar las cuentas de los usuarios que son nuevos o ya no hacen parte de la compañía.

• Los administradores de las diferentes plataformas de la compañía serán responsable de crear, cambiar, bloquear y eliminar las cuentas de los usuarios de los recursos tecnológicos o de los sistemas de información.

• Se debe garantizar procedimientos para la entrega de usuarios y contraseñas al personal interno de la compañía así mismo al personal que es externo o presta servicios subcontratados y que llegue a tener acceso a los servicios de red de la compañía.

• Se debe garantizar que los usuarios externos se conecten a una red WLAN diferente a la que están conectados los usuarios internos y que pertenecen a la compañía.

9.2 POLÍTICA DE PROTECCIÓN DE SOFTWARE MALICIOSO.

Los sistemas de información son vulnerables si no se cuenta con una política que establezca las disposiciones correspondientes para lograr la minimización del riesgo que se genera cuando no se tiene controlado este tipo de riesgo y se genera cuando un software malicioso como (virus, malware, etc), puede llegar a comprometer la confidencialidad, integridad y disponibilidad de la información de la empresa OBSS INGENIERÍA. Esta política de seguridad es importante y aplica para toda persona que tenga acceso autorizado y no autorizado a los servicios de red de la compañía. Para ello se debe tener en cuenta los siguientes ítems de esta política.

• El área (Oficina TI) encargada de la seguridad de la información de la compañía debe garantizar la implementación de los controles y medidas correspondientes a la seguridad en todos los ámbitos para prevenir y detectar y eliminar software que puedan afectar el triangulo de la seguridad de la información.

• Tanto el área de TI y RRHH debe culturizar a los usuarios internos para lanzar programas periódicos y actualizados sobre el riesgo y peligro que se puede ocasionar si se accede a un software malicioso y cuáles pueden ser los procedimientos para seguir para prevenir este tipo de inconvenientes.

• Se debe bloquear en los computadores que son entregados a los usuarios internos de la compañía tanto los puertos y la descarga de programa no autorizados para evitar que se instale cualquier software malicioso.

• Los usuarios internos de la compañía deben solicitar autorización a la mesa de servicios TI y es esta quién otorga permisos e instala el software que el usuario requiera y que este avalado para su uso.

• Se debe contar con sistemas de antivirus actualizados en todos los quipos informáticos de los usuarios internos de la compañía. Es responsable de esta política de seguridad el oficial de seguridad quien debe velar por los cumplimientos de esta política.

9.3 POLÍTICA DE COPIAS DE SEGURIDAD.

Esta política está orientada en la generación de copias de respaldo de los datos y el software de la compañía, donde se asigna los recursos necesarios, estableciendo los respectivos lineamientos de respaldo y almacenamiento de la información que sea prioridad de la compañía. Es importante tener claridad que esta política aplica para la información que está contenida en los servidores, es los equipos de cómputo de cada usuario interno de la compañía, de aplicativos y todo lo que contenga datos dentro de la compañía. Para ello es importante los siguientes ítems:

• El líder o jefe del área de TI es el único responsable de garantizar los procedimientos correspondientes para la identificación y la conservación de los datos o activos de la información.

• Los respaldos de la información deben ser solicitado por los jefes del área de TI y que de una u otra parte tienen responsabilidad de garantizar la continuidad, integridad y disponibilidad de la información.

• Se debe contar con un procedimiento claro al momento de llevar a cabo la solicitud de los respaldos y las copias a ejecutar para cada uno de los sistemas de información o los activos.

• Se debe garantizar con que periodicidad se llevarán a cabo los respaldos de los equipos de cómputo, de los servidores y demás activos de la compañía que contenga base de datos.

• Se debe garantizar la protección de los medios de respaldo la cual debe tener una custodia donde se garantice que la protección va a ser la más adecuada de todos los datos que se almacenan.

• Debe existir registros documentados, firmados y aprobados donde se especifique los procedimientos que se llevaron o el paso a paso de las copias de seguridad o el restablecimiento de estas.

• Se debe determinar con el jefe del área de TI cuál será el tiempo de conservación de la información. Los responsables del cumplimiento de esta política será el equipo de seguridad de la información de la compañía y la oficina de seguridad o TI de la compañía. 6. Política de configuraciones de Red. La política de gestión de configuración de red debe garantizar la organización y la actualización de todos los componentes de una red informática y la configuración de todos los equipos de red como Switches, router, firewalls, Access Point, Servidores, sistemas de detección de intrusos y otros dispositivos que hagan parte de la compañía. Todo debe ser documentado y respaldado por una copia de seguridad.

• Se debe garantizar que los equipos, activos de red cuenten con los parches de seguridad correspondientes y actualizados.

• Se debe contar con equipos de backup para garantizar la disponibilidad del servicio.

• Se debe contar con guardado de información en diferentes formatos y que sea de fácil acceso sobre la vida útil del equipo, tiempo de soporte, vencimiento de licencias, esto en pro de actuar de manera preventiva ante cualquier evento de cambio de activo.

• Se debe garantizar personal certificado y confiable que garantice los comandos correctos, instalaciones de actualización de los equipos y la transferencia de archivos y conocimiento para ser asertivos en las copias de seguridad correspondiente.

• Se debe tener documentado e inventariado las series, fabricante, funcionalidad, actualizaciones etc de los equipos para garantizar los procesos de auditoria internos.

Clasificacion	Detalle del Riesgo	Causas Generales	Efectos	Factor de impacto	Efectividad controles existentes	Frecuencia	Impacto	Nivel de Riesgo
Técnicos	Indisponibilidad del servicio	* Ataque DoS * Robo de equipos de transmisión * fallas en los nodos *Virus en los sistemas informaticos * No contar con sistema de seguridad por capas	*Incumplimiento contractuales y de ANS de los servicios prestados a usuarios Finales.	Tiempo	Moderado	Moderado	Alto	Alto
Técnicos	filtración y hurto de información	* Acceso de personas no autorizadas en las area de trabajo. * No cifrar la información * No contar con licencimientos requeridos para operar los servicios. * No bloquear puertos para la extracion de informacion * Contraseñas debiles * Ataques de fuerza bruta * Ataques de phising e ingenieria social * Ataques Ransowere	* Divulgación de información propia de la empresa OBSS.(Contratos, Compras, Facturaciones, Proveedores, nómina, etc) *Competencia aproveche información para los valores de los servicios para beneficios comerciales y financieros.	Beneficios	Bajo	Moderado	Alto	Alto
Técnicos	Acceso no autorizado a equipos de enrutamiento	* Habilitacion de acceso por Telnet * No contar con un servidor SSH para autenticar * No modificar los usuarios e IP acceso por default de fabricante.	* Generación de indisponibilidad del servicio. *Suplantación de MAC / IP, para el robo de información.	Calidad	Bajo	Alto	Alto	Crítico
Financiero	Incumplimiento de ANS pacatdos con clientes	* Fallas en la red * Factores climaticos * No contar con redudancia de los servicios	*Indisponibilidad de Servicio *Incumplimiento a la meta de los servicios o ANS. *Multas contractuales.	Costo	Bajo	Alto	Alto	Crítico
Judicial	Interferencia en el espectro radioelectrico por el uso de frecuencias no autorizadas por el MINITIC.	* No utilizar radios en banda licenciada. *No realizar análisis del espectro para garantizar un servicio optimo.	* Afectacion de servicios a terceros * Multas por uso inadecuado de las frecuencias. * Deficiencias en la calidad de los servicios suministrado a usuario final.	Calidad	Fuerte	Alto	Alto	Crítico
Técnicos	Riesgo de Robo en los NODOS de TX.	Robo de equipos (facilities) en cada uno de los NODOS.	* Indisponibilidad del Servicio *Perdida de los equipos de tx *Incurrir en penalizades del servicio prestado a empresas privadas. * Incumplimiento en los ANS.	Costo	Moderado	Moderado	Alto	Alto
Operativo	Riesgo de personal en sitio	Riesgo asociado a trabajo en Alturas	*Incumplimiento de las normas de seguridad. *Demanda por incumplimientos en los sistemas de seguridad. *	Costo	Fuerte	Moderado	Bajo	Bajo
Procedimental	Concepto de acto administrativo por parte de un o varios colaboradores a favor de un tercero.	Beneficio económico a favor de un o varios colaboradores.	*Manipulación de información propia de OBSS. *Trafico de influencias * Influencia de un tercero para obtener un concepto jurídico y/o acto administrativo a favor	Calidad	Fuerte	Bajo	Moderado	Bajo
Financiero	Ordenes de Pagos con soportes incompletos	*Incompleta entrega de soportes por parte del supervisor de contrato. *Inadecuada revisión de soportes por parte del área de tesorería.	* Sanciones de los proveedores por el pago incompleto. *Pérdida de beneficios por parte de los proveedores	Calidad	Fuerte	Bajo	Alto	Moderado

Ambiental	Contaminación por residuos en Sitios Rurales o estaciones BASE.	NO contar con politicas de manejo de residuos electricos, quimicos, en la fase de instalación y mantenimiento de Equipos en los NODOS.	*Indisponibilidad de Servicio *Incumplimiento a la meta de los servicios o ANS. *Cierre de NODO *Multas o cierre de NODO por parte de la corporación regional ambiental.	Calidad	Fuerte	Bajo	Moderado	Bajo
Operativo	Inadecuado control en la fase de implementación del contrato de servicios (usuario Final)	*Falta de seguimiento y control al contrato, incumplimiento de cronograma de implementación de servicios.	*retraso general al contrato. *Mayor costo operacional. *incumplimientos en cronograma a cliente final. *Disminución de Ingreso operacional.	Tiempo	Fuerte	Moderado	Alto	Alto
Operativo	Inadecuado control del contrato de servicios - Proveedor ISP.	Proveedor no garantice la disponibilidad del servicio en la ejecución del contrato.	*Indisponibilidad del Servicio a usuario Final. *inclumpliento de los ANS a usuario Final. *Penalizaciones por incumplimiento del servicio.	Calidad	Fuerte	Moderado	Alto	Alto

Tratamiento riesgo	Controles propuestos	Frecuencia	Impacto	Nivel de Riesgo Objetivo	Costo contingencia	RESPONSABLES
Mitigar	*Implementar una solución de seguridad en el centro de Datos y en la capa de tx. (fw perimetral, antivirus,IPS, IDS) *Garantizar varios sistemas de energía en los nodos para evitar indisponibilidad de servicio. *Disponer de seguridad en los Nodos, ya sea cercado electricos, camaras de seguridad etc.4	Alto	Bajo	Moderado	$ 91.995.540	Área de Seguridad OBSS
Aceptar	*Garantizar que los puertos USB esten bloqueados en los equipos de cada uno de los colaboradores de la empresa. *Definir una matriz de roles y responsabilidades para la gestión de la información. * Definiir los procesos de asignación y privilegios de usuario. *Culturizar a los colaboradores en no dejar los computadores sin bloqueo cuando no estan en su sitio de trabajo. *Implementar un sistema CCTV para nodo principal y las oficinas de trabajo.	Bajo	Alto	Moderado	$ 118.483.000	Área de TI de OBSS
Evitar	* Implementar autenticación a traves de un Servidor SSH. *Cambiar las contraseñas y las IP de ingreso de acceso local que entregan los fabricantes. *Comprar licenciamientos de seguridad que permita cifrar la información.	Moderado	Moderado	Moderado	$ 21.000.000	Área de Seguridad de OBSS
Mitigar	* Realizar mantenimientos preventivos y correctivos sobre la infraestructrura. * Disponibilidad de equipos de Backup para cuando exista contingencias de robo. * Garantizar calidad en la implementación de los servicios. * Contar con procesos la gestión de incidentes.	Bajo	Moderado	Bajo	$ -	Área de Redes OBSS
Mitigar	* Realizar estudios o análisis del uso correcto del espectro radioelectrico. * Adquisición de Radios licenciados. * Trámite de permisos para el uso de la frecuencia en el espectro con el MINTIC.	Moderado	Moderado	Moderado	$ 12.500.000	Área de Redes OBSS
Mitigar	* Realizar una buena protección de los NODOS a nivel de seguridad física *Implementar un sistema CCTV para nodo principal y las oficinas de trabajo.	Moderado	Bajo	Bajo	$ 19.383.000	Área de TI de OBSS
Mitigar	*Garantizar al personal la respectiva dotación y los EPP. *Mantener actualizados las certificaciones de trabajo en Alturas.	Bajo	Bajo	Insignificante	$ -	Área de HSEQ
Mitigar	*Realizar los controles y capacitaciones de ética y cumplimiento para que los colaboradores se cultiricen en la importancia de no aceptar beneficios por terceros.	Bajo	Bajo	Insignificante	$ 5.000.000	Área de RRHH de OBSS
Mitigar	* Realizar Lista de Chequeo de los contratos y los pagos correspondientes según procedimiento de la cuenta por pagar a cada proveedor. * Capacitación a personal desde el área de contratos y tesorería. Seguimiento a las cuentas de ordenes de pago por parte del área de tesorería.	Bajo	Bajo	Insignificante	$ -	Área de Tesorería OBSS

Mitigar	* Realizar la correcta disposición de los residuos generados en la instalación de equipos, cables, Banco de baterias etc. *Contar con una politica Ambiental para tratamiento de riesgos quimicos, solidos, electricos etc.	Bajo	Moderado	Bajo	$ 6.000.000,00	Área de Redes OBSS
Mitigar	*Seguimiento semanal del contrato *Segumiento de contrato incluyendo actividades y áreas responsables. *Asignación de Gerente de Servicios - Proyectos para identificar, gestionar, cumplir las etapas de implementación.	Moderado	Moderado	Moderado	$ 7.500.000	Área de RRHH de OBSS Área de Proyectos OBSS
Evitar	*Contar con un canal alterno para garantizar la disponibilidad del Servicio a los usuarios finales. *Pactando ANS, multas y penalidades con los proveedores de Servicio IPS.	Moderado	Moderado	Moderado	$ 11.120.000	Área de Redes OBSS
					$ 292.981.540	

TABLAS DE VALORACIÓN DE CONTROLES, FRECUENCIA E IMPACTOS

TABLA DE VALORACIÓN DE CONTROLES

DESCRIPTOR	DEFINICIÓN
Fuerte	Se han adoptado todos o la mayoría de los controles económicamente viables y el conjunto de controles que mitigan el riesgo están correctamente diseñados y funcionan adecuadamente
Moderado	El conjunto de controles aplicados presentan algunas debilidades en cuanto a su diseño y/o ejecución o no permiten una gestión adecuada de todos los sucesos potenciales del riesgo.
Bajo	El conjunto de controles no permite mitigar el riesgo o se desconocen los controles de mitigación.

*Diseño: Cuenta con responsable asignado, documentación y periodicidad definida
*Ejecución o funcionamiento: Es medido y se cuenta con evidencias de su ejecución

TABLA DE FRECUENCIA

DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA CORPORATIVA
Alto	Se sabe que el caso ocurrirá en la mayoría de las circunstancias	Riesgos cuya probabilidad de ocurrencia es **muy alta**, es decir, se tiene alto grado de seguridad de que esté presente >50%
Moderado	Suceso que se presenta con cierta regularidad	Riesgos cuya probabilidad de ocurrencia es **alta,** es decir, se tiene entre un 20% y un 50% de seguridad de que esté presente
Bajo	Suceso inhabitual	Riesgos cuya probabilidad de ocurrencia es **baja,** es decir, se tiene menor a 20% de seguridad de que esté presente

TABLA DE VALORACIÓN DE IMPACTO

Impacto	Bajo	Moderado	Alto
ALCANCE	La modificación del alcance es apenas perceptible	La modificación del alcance afecta las principales áreas pero es aceptado por el Patrocinador y/o Cliente	La modificación del alcance es inaceptable para el Patrocinador y/o Cliente
TIEMPO	Atraso menor al 11%	Atraso entre el 11 y 20%	Atraso superior al 20%
CALIDAD	Degradación de la calidad, apenas perceptible	La reducción de la calidad, requiere la aprobación del Patrocinador y/o Cliente	Reducción de la calidad, inaceptable para el Patrocinador y/o Cliente
COSTO	Sobrecosto menor al 3% del presupuesto del proyecto Erosión del presupuesto menor al 3%	Sobrecosto máximo entre el 3% y 5% del presupuesto del proyecto Erosión del presupuesto entre 3% y 5%	Sobrecosto máximo del 5% del presupuesto del proyecto Erosión del presupuesto mayor al 5%

Impacto Financiero	Beneficios		Impacto Financiero	Beneficios	
$ 0		>20% Impacto Alto	$ 0		<80% Impacto Alto
$ 0	$ 0	11% - 20% Impacto Moderado	$ 0	$ 0	80% - 90% Impacto Moderado
$ 0		<11% Impacto Bajo	$ 0		>90% Impacto Bajo

PONER VALOR DEL PROYECTO COSTO-BENEFICIO

NIVEL DE RIESGO	VALORACIÓN DEL CONTROL
Crítico y Alto	Fuerte
	Moderado
	Bajo
Moderado	Fuerte
	Moderado

	Bajo
Bajo	Cualquier nivel
Insignificante	Cualquier nivel

CRITERIOS DE ACEPTABILIDAD

CRITERIO

El riesgo se encuentra en un nivel que exige **monitoreo permanente** del entorno, **no es necesario tomar medidas de control adicionales** a las existentes.
Se implementarán nuevos controles si y solo si existe un criterio no discrecional que obligue su implementación
Deberá ser gestionado y monitoreado por el **responsable del riesgo** y el **superior inmediato**

Se deben tomar acciones para mejorar los controles existentes y/o implementar nuevos controles, estas acciones se deben tomar en el **corto plazo** (puede esperar hasta el año siguiente o hasta que pueda presupuestarse) y pueden implicar recursos adicionales en el proyecto. Es necesario definir el nivel de riesgo objetivo (identificando si disminuiría la frecuencias, el impacto o ambos) para el período siguiente de evaluación.
Deberá ser gestionado y monitoreado por el **responsable del riesgo y el superior inmediato**

Se deben tomar acciones para mejorar los controles existentes y/o implementar nuevos controles de **forma inmediata**, la intervención en este nivel de riesgo es de alta prioridad y pueden implicar recursos adicionales en el proyecto. Es necesario definir el nivel de riesgo objetivo (identificando si disminuiría la frecuencias, el impacto o ambos) para el período siguiente de evaluación.
Deberá ser gestionado y monitoreado por el responsable del riesgo y el superior inmediato

El riesgo se encuentra en un nivel que exige **monitoreo permanente** del entorno, **no es necesario tomar medidas de control adicionales** a las existentes.
Se implementarán nuevos controles si y solo si existe un criterio no discrecional que obligue su implementación
Deberá ser gestionado y monitoreado por el **responsable del riesgo**

Se deben tomar acciones para **mejorar los controles existentes** y/o implementar nuevos controles, estas acciones se deben tomar en el **mediano plazo** (no debe exceder a 2 años) y debe realizarse con los recursos ordinarios del proyecto. Queda a consideración del Responsable, de acuerdo con la evaluación del contexto, costos y tendencias del riesgo, definir el nivel de riesgo objetivo (identificando si disminuiría la frecuencias, el impacto o ambos) para el período siguiente de evaluación.
Se implementarán nuevos controles si y solo si existe un criterio no discrecional que obligue su implementación
Deberá ser gestionado y monitoreado por el responsable del riesgo

Se deben tomar acciones para **mejorar** los controles existentes y/o implementar nuevos controles, estas acciones se deben tomar en el **corto plazo** (puede esperar hasta el año siguiente o hasta que pueda presupuestarse) y debe realizarse con los recursos ordinarios del proyecto. Queda a consideración del Responsable, de acuerdo con la evaluación del contexto, costos y tendencias del riesgo, definir el nivel de riesgo objetivo (identificando si disminuiría la frecuencias, el impacto o ambos) para el período siguiente de evaluación.
Se implementarán nuevos controles si y solo si existe un criterio no discrecional que obligue su implementación
Deberá ser gestionado y monitoreado por el responsable del riesgo

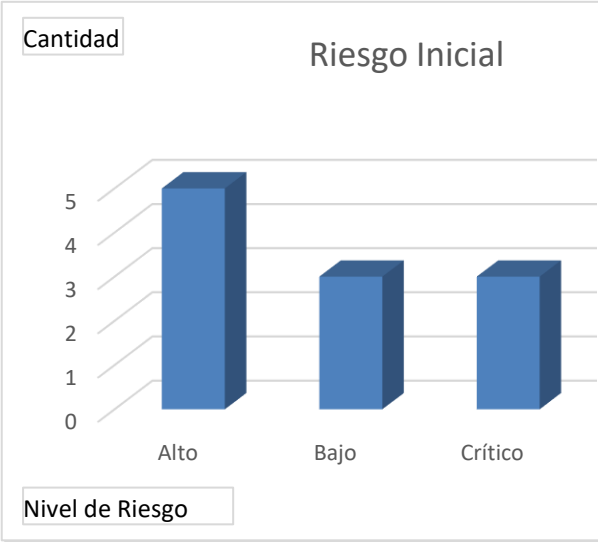
El riesgo se encuentra en un nivel que **puede asumirse** sin necesidad de tomar otras medidas de control diferentes a las existentes. Queda **a consideración del Responsable**, de acuerdo con la evaluación del contexto, costos y tendencias del riesgo, **definir el nivel de riesgo objetivo** (identificando si disminuiría la frecuencias, el impacto o ambos) para el período siguiente de evaluación.
Se implementarán nuevos controles si y solo si existe un criterio no discrecional que obligue su implementación
Deberá ser gestionado y monitoreado por el **responsable del riesgo** para que **no incremente su nivel**

El riesgo se encuentra en un nivel que **puede asumirse** sin necesidad de tomar otras medidas de control diferentes a las existentes.
Se implementarán nuevos controles si y solo si existe un criterio no discrecional que obligue su implementación
Deberá ser gestionado y monitoreado por el **responsable del riesgo** para que **no incremente su nivel**

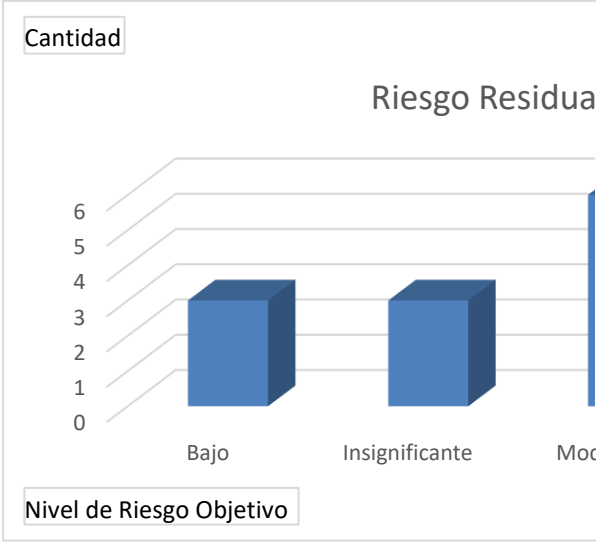
Solución	Ubicación	Cantidad
Firewall NGFW 600 E HA	Nodo principal	2
CÁMARA TIPO BALA 1080P	Nodos	30
Gabinete	Nodos	30
NVR (4 canales)	Nodos	1
Camaras tipo domo	Nodo principal	15
NVR (16) POE	Nodo principal	1
Disco duro 1TB	Nodo principal	1
Cable UPT (100 m)	Nodo principal	1
Conector RJ45	Nodo principal	20
Canaleta (100 m)	Nodo principal	1
Rack (gabinete)	Nodo principal	1
UPS (2 KVAs)	Nodo principal	31
Cable HMI	Nodo principal	10
pantallas de 43"	Nodo principal	5
Servidor SSH	Nodo principal	1
Servicios profesionales (50 horas)	Nodo principal	50
Canales alternos de intenet 10G	Nodo principal	2
Permisos Mintic uso espectro	Todos los nodos	1
Capacitaciones	Nodo principal	1
Tratamiento de residuos	Todos los nodos	1
TOTAL		

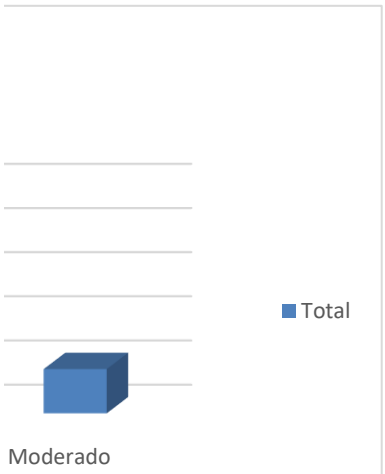
PRESUPUESTO		Total
Opex	Capex	
	$ 45.997.770	$ 91.995.540,00
	$ 750.000	$ 750.000,00
	$ 600.000	$ 18.000.000,00
	$ 633.000	$ 633.000,00
	$ 5.841.000	$ 5.841.000,00
	$ 13.890.000	$ 13.890.000,00
	$ 302.000	$ 302.000,00
	$ 256.000	$ 256.000,00
	$ 100.000	$ 2.000.000,00
	$ 100.000	$ 100.000,00
	$ 10.560.000	$ 10.560.000,00
	$ 79.484.000	$ 79.484.000,00
	$ 50.000	$ 50.000,00
	$ 6.000.000	$ 6.000.000,00
	$ 21.000.000	$ 21.000.000,00
$ 7.500.000		$ 7.500.000,00
$ 5.560.000		$ 11.120.000,00
$ 12.500.000		$ 12.500.000,00
$ 5.000.000		$ 5.000.000,00
$ 6.000.000		$ 6.000.000,00
$ 36.560.000	$ 185.563.770	$ 292.981.540

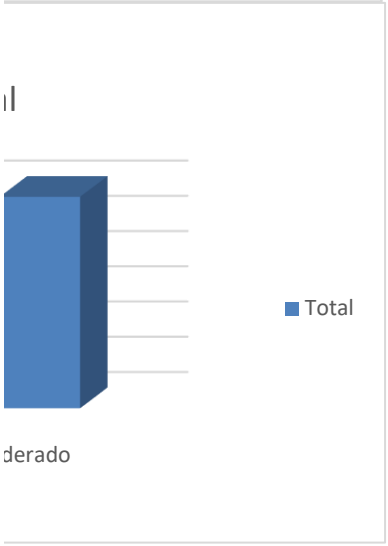
Nivel del riesgo	Cantidad
Alto	5
Bajo	3
Crítico	3
Moderado	1
Total general	**12**



Nivel del riesgo	Cantidad
Bajo	3
Insignificante	3
Moderado	6
Total general	**12**




Total
Moderado


Total
derado

ISO 27001 SOA (Statement of Applicability)

Estado	Significado
Cumple satisfactoriamente	Existe, es gestionado, se está cumpliendo con lo que la norma solicita, está documentado, es conocido y aplicado por todos los involucrados en el SGSI. cumple 100%.
Cumple parcialmente	Lo que la norma requiere se está haciendo de manera parcial, se está haciendo diferente, no está documentado, se definió pero no se gestiona.
No cumple	No existe y/o no se está haciendo.
No aplica	El control no es aplicable para la entidad. En el campo evidencia por favor indicar la justificación respectiva de su no aplicabilidad.

CONTROLES ANEXO A NORMA ISO 27001			ESTADO	REFERENCIA
A5	POLÍTICAS DE LA SEGURIDAD DE LA INFORMACION			
A5.1	Orientación de la dirección para la gestión de la seguridad de la información			
Objetivo: Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes				
A5.1.1	Políticas para la seguridad de la información	Control: Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.	No cumple	No se tiene implementada una politica de seguridad de la informacion.
A5.1.2	Revisión de las políticas para la seguridad de la información.	Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.	No cumple	No se tiene implementada una politica de seguridad de la informacion.
A6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION			
A6.1	Organización interna			
Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.				
A6.1.1	Roles y responsabilidades para la seguridad de la información	Control: Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	No cumple	No se tiene definida una matriz de roles y responsabilidad en la seguridad de la informacion. Se recomienda involucrar a los directivos de la compañía.
A6.1.2	Separación de deberes	Control: Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización	No cumple	No se tiene definida una estructura con las responsabilidades por areas de la compañía.
A6.1.3	Contacto con las autoridades	Control: Se deben mantener contactos apropiados con las autoridades pertinentes.	Cumple parcialmente	OBSS tienen identificadas las autoridades relacionadas con el cumplimiento de la ley.
A6.1.4	Contacto con grupos de interés especial	Control: Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad	No cumple	OBSS no se tiene contacto con entidades o profesionales de la seguridad de la informacion.
A6.1.5	Seguridad de la información en la gestión de proyectos.	Control: La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.	No cumple	No se tiene definido un proceso para el tratamiento de la informacion relacionada con los proyectos.
A6.2	Dispositivos móviles y teletrabajo			
Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles				
A6.2.1	Política para dispositivos móviles	Control: Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	No aplica	No tienes definida una politica para la seguridad de la informacion de la organización a traves de los dispositivos moviles
A6.2.2	Teletrabajo	Control: Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	No aplica	No tienes definida una politica para la seguridad de la informacion de la organización para el escenario de teletrabajo.
A7	SEGURIDAD DE LOS RECURSOS HUMANOS			
A7.1	Antes de asumir el empleo			
Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.				
A7.1.1	Selección	Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso y a los riesgos percibidos.	Cumple parcialmente	La organización verifica los antecendentes de los candidatos que se presentan a un cargo de acuerdo con las leyes, reglamentaciones y etica pertinentes.
A7.1.2	Términos y condiciones del empleo	Control: Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	No cumple	Actualmente OBSS no tiene
A7.2	Durante la ejecución del empleo			
Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.				

A7.2.1	Responsabilidades de la dirección	Control: La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	No cumple	No se tiene implementada una politica de seguridad de la informacion.
A7.2.2	Toma de conciencia, educación y formación en la seguridad de la información.	Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.	No cumple	No se tiene implementada una politica de seguridad de la informacion.
A7.2.3	Proceso disciplinario	Control: Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	No cumple	No se tiene implementada una politica de seguridad de la informacion.
A7.3	Terminación y cambio de empleo			
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo				
A7.3.1	Terminación o cambio de responsabilidades de empleo	Control: Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir.	No cumple	No se tiene definida una politica para la seguridad de la informacion luego de la terminacion o cambio de empleo.
A8	GESTION DE ACTIVOS			
A8.1	Responsabilidad por los activos			
Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección adecuadas.				
A8.1.1	Inventario de activos	Control: Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	No cumple	No se cuenta con un inventario de activos.
A8.1.2	Propiedad de los activos	Control: Los activos mantenidos en el inventario deben tener un propietario.	No cumple	No se cuenta con un inventario de activos y no tiene definido un propietario.
A8.1.3	Uso aceptable de los activos	Control: Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	No cumple	No se tiene implementada una politica de seguridad de la informacion.
A8.1.4	Devolución de activos	Control: Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	Cumple parcialmente	No se tiene definido un proceso para la devolucion de activos en los casos de terminacion de contrato.
A8.2	Clasificación de la información			
Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.				
A8.2.1	Clasificación de la información	Control: La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	No cumple	No se tiene identificada la informacion confidencial y no se realiza la clasificacion y tratamiento correpondiente.
A8.2.2	Etiquetado de la información	Control: Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.	No cumple	No se tiene establecido un procedimiento para el etiquetado de informacion digital o impresa.
A8.2.3	Manejo de activos	Control: Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	No cumple	No se tiene implementada una politica de seguridad de la informacion.
A8.3	Manejo de medios			
Objetivo: Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios				
A8.3.1	Gestión de medios removibles	Control: Se deben implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	No cumple	No se tienen implantados mecanismos que controlen el acceso a medios de almacenamiento removibles.
A8.3.2	Disposición de los medios	Control: Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	No cumple	No se tiene establecido un procedimiento formal para la disposicion de medios.
A8.3.3	Transferencia de medios físicos	Control: Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	No cumple	No se tiene resguardo de medios con terceros.
A9	CONTROL DE ACCESO			
A9.1	Requisitos del negocio para el control de acceso			
Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.				
A9.1.1	Política de control de acceso	Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la seguridad de la información.	No cumple	No tiene definida una politica de control de acceso.
A9.1.2	Acceso a redes y a servicios en red	Control: Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	Cumple parcialmente	Se tiene definido privilegios para ciertos usuarios
A9.2	Gestión de acceso de usuarios			
Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.				

A9.2.1	Registro y cancelación del registro de usuarios	Control: Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	No cumple	No cuenta con un proceso para el registro y baja de usuarios.
A9.2.2	Suministro de acceso de usuarios	Control: Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.	No cumple	No cuenta con un proceso para el registro y baja de usuarios.
A9.2.3	Gestión de derechos de acceso privilegiado	Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.	No cumple	No se cuenta con un proceso para restringir y controlar el acceso a la red
A9.2.4	Gestión de información de autenticación secreta de usuarios	Control: La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	No cumple	No se tiene definido un proceso para la autenticacion secreta
A9.2.5	Revisión de los derechos de acceso de usuarios	Control: Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	Cumple parcialmente	Los dueños de los activos revisan permanentente los derechos de acceso de los usarios.
A9.2.6	Retiro o ajuste de los derechos de acceso	Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	Cumple parcialmente	Se limita el acceso de los usuarios de personas que terminan su contrato laboral.
A9.3	Responsabilidades de los usuarios			
Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.				
A9.3.1	Uso de información de autenticación secreta	Control: Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	No cumple	No cuenta con un herramienta de autenticacion.
A9.4	Control de acceso a sistemas y aplicaciones			
Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.				
A9.4.1	Restricción de acceso a la información	Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	Cumple parcialmente	Se controlan los permisos de acceso otorgados a los usuarios pero no se tiene establecido un procedimiento formal.
A9.4.2	Procedimiento de ingreso seguro	Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	No cumple	No se cuenta con un metodo de autenticacion de ingreso seguro.
A9.4.3	Sistema de gestión de contraseñas	Control: Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	No cumple	No se cuenta con una herramienta que defina una politica de calidad de contraseñas
A9.4.4	Uso de programas utilitarios privilegiados	Control: Se debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.	No cumple	No hay controles para la ejecucion de programas que puedan anular las funciones del sistema.
A9.4.5	Control de acceso a códigos fuente de programas	Control: Se debe restringir el acceso a los códigos fuente de los programas.	No aplica	Los software utilizados son propiamente de fabricantes y no permite el acceso a los codigos fuente.
A10	CRIPTOGRAFIA			
A10.1	Controles criptográficos			
Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o la integridad de la información				
A10.1.1	Política sobre el uso de controles criptográficos	Control: Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	No cumple	No se tiene definida una politica sobre el uso de controles criptograficos.
A10.1.2	Gestión de llaves	Control: Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.	No aplica	No se tiene definida una politica sobre el uso, proteccion y tiempo de vida de las llaves criptograficas.
A11	SEGURIDAD FISICA Y DEL ENTORNO			
A11.1	Áreas seguras			
Objetivo: Prevenir el acceso físico no autorizado, el daño e la interferencia a la información y a las instalaciones de procesamiento de información de la organización.				
A11.1.1	Perímetro de seguridad física	Control: Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o critica, e instalaciones de manejo de información.	No cumple	No se tienen definidos perimetros de seguridad.
A11.1.2	Controles de acceso físicos	Control: Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.	No cumple	No se tiene un proceso ni una herramienta para garantizar el control de acceso.
A11.1.3	Seguridad de oficinas, recintos e instalaciones.	Control: Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones..	Cumple parcialmente	Se cuenta con seguridad fisica para las oficinas e instalaciones pero no se tiene definido un proceso.
A11.1.4	Protección contra amenazas externas y ambientales.	Control: Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	No cumple	No hay un procedimiento establecido como plan de continuidad del negocio, frente a desastres naturales.
A11.1.5	Trabajo en áreas seguras.	Control: Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.	No cumple	No hay un proceso establecido para trabajo en zonas seguras.
A11.1.6	Áreas de carga, despacho y acceso público	Control: Se deben controlar los puntos de acceso tales como las áreas de despacho y carga y otros puntos por donde pueden entrar personas no autorizadas y, si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	No cumple	No se tiene un proceso para restringir area de despacho y carga.
A11.2	Equipos			
Objetivo: Prevenir la perdida, daño, robo o compromiso de activos y la interrupción de las operaciones de la organización.				

A11.2.1	Ubicación y protección de los equipos	Control: Los equipos deben de estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.	Cumple parcialmente	Los equipos estan aislados pero no se tiene un proceso para evitar el acceso a personas no autorizadas.
A11.2.2	Servicios de suministro	Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	Cumple satisfactoriamente	Los equipos se encuentran protegidos con UPS y banco de baterias.
A11.2.3	Seguridad en el cableado.	Control: El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.	Cumple parcialmente	Se cuenta con cableado estructurado implementado pero no cumple con los estadares de la industria.
A11.2.4	Mantenimiento de los equipos.	Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Cumple parcialmente	Se cuenta con un plan de mantenimiento preventivo y correctivo, pero no esta documentado.
A11.2.5	Retiro de activos	Control: Los equipos, información o software no se deben retirar de su sitio sin autorización previa.	Cumple satisfactoriamente	No se tiene definido un proceso para el retiro de equipos.
A11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Control: Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	No cumple	No se tiene establecido un procedimiento de seguridad para los equipos fuera de la organización, no se tiene seguro contra robo y la infraestructura esta expuesta a la intemperie.
A11.2.7	Disposición segura o reutilización de equipos	Control: Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobreescrito en forma segura antes de su disposición o reúso.	No cumple	No se tiene establecido un proceso ni se cuenta con las herramientas para garantizar un borrado seguro.
A11.2.8	Equipos de usuario desatendido	Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	No cumple	No se ha concientizado a los usuarios sobre las buenas practicas al momento de dejar sus estciones de trabajo activas.
A11.2.9	Política de escritorio limpio y pantalla limpia	Control: Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.	No cumple	No se cuenta con una politica de escritorio limpio.
A12	SEGURIDAD DE LAS OPERACIONES			
A12.1	Procedimientos operacionales y responsabilidades			
Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.				
A12.1.1	Procedimientos de operación documentados	Control: Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.	No cumple	No hay documentacion de los procesos del negocio.
A12.1.2	Gestión de cambios	Control: Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	No cumple	No hay proceso de control de cambios.
A12.1.3	Gestión de capacidad	Control: Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.	No cumple	La capacidad se va dimesionando en la medida de la necesidad.
A12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Control: Se deben separar los ambientes de desarrollo, pruebas y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	No aplica	No se hace desarrollo de software en la compañía.
A12.2	Protección contra códigos maliciosos			
Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.				
A12.2.1	Controles contra códigos maliciosos	Control: Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	Cumple parcialmente	Solo se cuenta con antivirus
A12.3	Copias de respaldo			
Objetivo: Proteger contra la perdida de datos				
A12.3.1	Respaldo de la información	Control: Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	Cumple parcialmente	Se realizan copias de respaldo en discos externos.
A12.4	Registro y seguimiento			
Objetivo: Registrar eventos y generar evidencia				
A12.4.1	Registro de eventos	Control: Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	No cumple	No se tiene establecido un procedimiento para la auditoria de los logs de eventos de servidores y equipos.
A12.4.2	Protección de la información de registro	Control: Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	No cumple	No se protege la integridad de los archivos de log.
A12.4.3	Registros del administrador y del operador	Control: Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.	No cumple	No se tiene establecido un procedimiento para la auditoria de los logs de eventos.
A12.4.4	Sincronización de relojes	Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	Cumple satisfactoriamente	No se cuenta con un sistema qe sincronice los relojes de los equipos que se usan en la organización.
A12.5	Control de software operacional			

Objetivo: Asegurarse de la integridad de los sistemas operacionales				
A12.5.1	Instalación de software en sistemas operativos	Control: Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	Cumple parcialmente	No se tienen definidos los privilegios para los usuarios para controlar la instalacion de software en los equipos.
A12.6	Gestión de la vulnerabilidad técnica			
Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas				
A12.6.1	Gestión de las vulnerabilidades técnicas	Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	No cumple	No se ha realizado una prueba de analisis de vulnerabilidades.
A12.6.2	Restricciones sobre la instalación de software	Control: Se deben establecer e implementar las reglas para la instalación de software por parte de los usuarios.	No cumple	No se tiene implementada una politica de seguridad de la informacion.
A12.7	Consideraciones sobre auditorias de sistemas de información			
Objetivo: Minimizar el impacto de las actividades de auditoria sobre los sistemas operativos				
A12.7.1	Controles de auditorías de sistemas de información	Control: Los requisitos y actividades de auditoria que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	No aplica	OBSS no se somete actualmente a procedimientos de auditoria interna o externa.
A13	SEGURIDAD DE LAS COMUNICACIONES			
A13.1	Gestión de la seguridad de las redes			
Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.				
A13.1.1	Controles de redes	Control: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	No cumple	No se tiene ninguna restricion de conexión hacia red WIFI
A13.1.2	Seguridad de los servicios de red	Control: Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.	No cumple	El acceso a los servicios de red no estan limitadoa a los usuarios.
A13.1.3	Separación en las redes	Control: Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	No cumple	No se tienen segregadas las redes, los sistemas de informacion y la red de usuarios hacen parte de la misma red.
A13.2	Transferencia de información			
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.				
A13.2.1	Políticas y procedimientos de transferencia de información	Control: Se debe contar con políticas, procedimientos y controles de transferencia información formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.	Cumple parcialmente	Para la transferencia de informacion en los radio enlaces se implementan tecnicas de cifrado propios de los equipos.
A13.2.2	Acuerdos sobre transferencia de información	Control: Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.	Cumple parcialmente	Se aprovechan las protecciones a la informacion que ofrece el correo de gmail y para la trasfeencia de datos los metodos de cifrado y
A13.2.3	Mensajería Electronica	Control: Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	Cumple parcialmente	Se aprovechan las protecciones a la informacion que ofrece el correo de gmail.
A13.2.4	Acuerdos de confidencialidad o de no divulgación	Control: Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	Cumple parcialmente	Se hace uso de acuerdos de confidencialidad con miembros de la organización ni terceros.
A14	Adquisición, desarrollo y mantenimiento de sistemas			
A14.1	Requisitos de seguridad de los sistemas de información			
Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes .				
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Control: Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	No cumple	En el momento de adquirir/renovar el software no se consultan los requisitos de seguridad.
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	Control: La informacion involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	Cumple parcialmente	No se cuenta con una herramienta para la proteccion de la informacion que viaja sobre redes publicas, solomente con funcionalidades de seguridad implicitas en las aplicaciones que se
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones.	Control: La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.	Cumple parcialmente	Se cuenta unicamnete con las herramientas proteccion propias de las aplicaciones y en caso de los radio enlaces con los protocolo de trasmision de datos y los metodos de proteccion propias de fabricante.
A14.2	Seguridad en los procesos de Desarrollo y de Soporte			
Objetivo: Asegurar que la seguridad de la información este diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.				

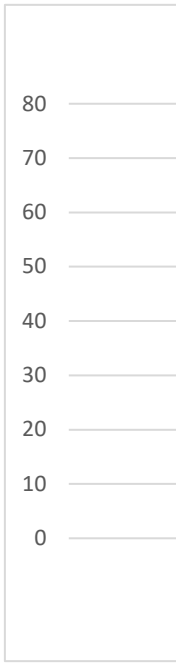
A.14.2.1	Política de desarrollo seguro	Control: Se debe establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.	No aplica	No se hace desarrollo de software en la compañía.
A.14.2.2	Procedimientos de control de cambios en sistemas	Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.	No aplica	No se hace desarrollo de software en la compañía.
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Control: Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.	No aplica	No se hace desarrollo de software en la compañía.
A.14.2.4	Restricciones en los cambios a los paquetes de software	Control: Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	No aplica	No se hace desarrollo de software en la compañía.
A.14.2.5	Principio de Construcción de los Sistemas Seguros.	Control: Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	No aplica	No se hace desarrollo de software en la compañía.
A.14.2.6	Ambiente de desarrollo seguro	Control: Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	No aplica	No se hace desarrollo de software en la compañía.
A.14.2.7	Desarrollo contratado externamente	Control: La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	No aplica	No se hace desarrollo de software en la compañía.
A.14.2.8	Pruebas de seguridad de sistemas	Control: Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.	No aplica	No se hace desarrollo de software en la compañía.
A.14.2.9	Prueba de aceptación de sistemas	Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.	No aplica	No se hace desarrollo de software en la compañía.
A14.3	Datos de prueba			
Objetivo: Asegurar la protección de los datos usados para pruebas.				
A.14.3.1	Protección de datos de prueba	Control:Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.	No aplica	No se hace desarrollo de software en la compañía.
A15	RELACIONES CON LOS PROVEEDORES			
A15.1	Seguridad de la información en las relaciones con los proveedores.			
Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.				
A15.1.1	Política de seguridad de la información para las relaciones con proveedores	Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar.	No cumple	No se tienen acuerdos de confidencialidad con terceros.
A15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Control: Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.	No cumple	No se tienen acuerdos de confidencialidad con terceros.
A15.1.3	Cadena de suministro de tecnología de información y comunicación	Control: Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.	No cumple	No se tienen acuerdos formales con terceros y proveedores.
A15.2	Gestión de la prestación de servicios de proveedores			
Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores				
A15.2.1	Seguimiento y revisión de los servicios de los proveedores	Control: Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	No cumple	No se tiene establecido un control o seguimiento a los ANS de los distintos proveedores.
A15.2.2	Gestión del cambio en los servicios de los proveedores	Control: Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y las mejoras de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos de negocio involucrados, y la reevaluación de los riesgos.	No cumple	No se tiene establecido un control o seguimiento a los ANS de los distintos proveedores.
A16	GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION			
A16.1	Gestión de incidentes y mejoras en la seguridad de la información			
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.				
A16.1.1	Responsabilidades y procedimientos	Control: Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	No cumple	No se tiene establecido un procedimiento para la gestion de incidentes de seguridad de la informacion.
A16.1.2	Reporte de eventos de seguridad de la información	Control: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.	No cumple	No se cuenta con una herramienta con los canales apropiados para informar los eventos de seguridad.

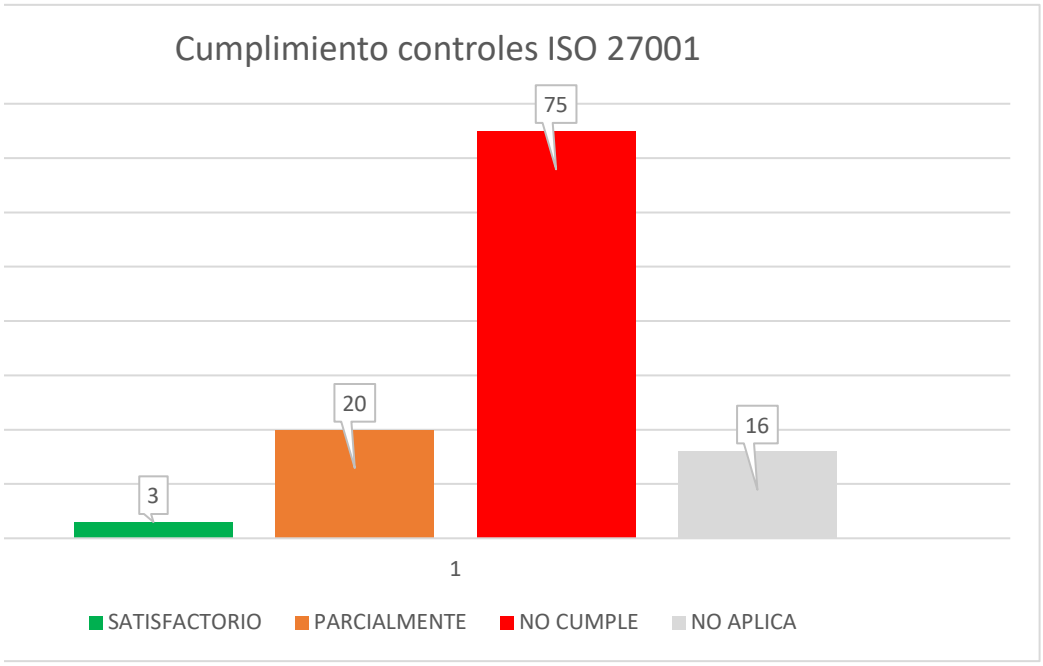
A16.1.3	Reporte de debilidades de seguridad de la información	Control: Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	No cumple	No se tiene establecido un procedimiento para la gestion de incidentes de seguridad de la informacion.
A16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Control: Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.	No cumple	No se tiene establecido un procedimiento para la gestion de incidentes de seguridad de la informacion.
A16.1.5	Respuesta a incidentes de seguridad de la información	Control: Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	No cumple	No se tiene establecido un procedimiento para la gestion de incidentes de seguridad de la informacion.
A16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o impacto de incidentes futuros.	No cumple	No se tiene establecido un procedimiento para la gestion de incidentes de seguridad de la informacion.
A16.1.7	Recolección de evidencia	Control: La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	No cumple	No se tiene establecido un procedimiento para la gestion de incidentes de seguridad de la informacion.
A17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD DE NEGOCIO			
A17.1	Continuidad de Seguridad de la información			
Objetivo: La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.				
A17.1.1	Planificación de la continuidad de la seguridad de la información	Control: La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	No cumple	No se tiene implementado un plan de continuidad del negocio
A17.1.2	Implementación de la continuidad de la seguridad de la información	Control: La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	No cumple	No se tiene implementado un plan de continuidad del negocio
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Control: La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.	No cumple	No se tiene implementado un plan de continuidad del negocio
A17.2	Redundancias			
Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.				
A17.2.1	Disponibilidad de instalaciones de procesamiento de información	Control: Las instalaciones de procesamientos de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	No cumple	No se cuenta con un centro de datos alterno en caso de que la sede principal se vea afectada y no pueda soportar la operación.
A18	CUMPLIMIENTO			
A18.1	Cumplimiento de requisitos legales y contractuales			
Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.				
A18.1.1	Identificación de la legislación aplicable.	Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.	No cumple	No se tiene identificada las leyes y normas que aplican a la organización y el negocio.
A18.1.2	Derechos propiedad intelectual (DPI)	Control: Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.	No cumple	No se tiene implementado un proceso que cumpla con los requisitos legislativos, de reglamentacion contra los derechos de propiedad intelectual, algunos de los software que usa OBSS no son licenciados.
A18.1.3	Protección de registros	Control: Los registros se deben proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	No cumple	No se cuenta con registros del licenciamiento.
A18.1.4	Privacidad y protección de información de datos personales	Control: Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable.	No cumple	No se cuenta con un sistema para la proteccion de informacion de datos personales.
A18.1.5	Reglamentación de controles criptográficos.	Control: Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	No cumple	No se tiene implementados controles criptograficos.
A18.2	Revisiones de seguridad de la información			
Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.				
A18.2.1	Revisión independiente de la seguridad de la información	Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información), se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.	No cumple	No se tiene establecida una politica de seguridad de la informacion.
A18.2.2	Cumplimiento con las políticas y normas de seguridad	Control: Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.	No cumple	No se tiene establecida una politica de seguridad de la informacion.

A18.2.3	Revisión del cumplimiento técnico	Control: Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	No cumple	No se tiene establecida una politica de seguridad de la informacion.
Fuente: NTC-ISO-IEC 27001:2013				

Cumple satisfactoriamente
Cumple parcialmente
No cumple
No aplica

CUMPLIMIENTO			
SATISFACTORIO	PARCIALMENTE	NO CUMPLE	NO APLICA
3	20	75	16




Cumplimiento controles ISO 27001
75
20
16
3
1
SATISFACTORIO
PARCIALMENTE
NO CUMPLE
NO APLICA

0.65789474

Etiquetas de fila	Cuenta de ESTADO
No cumple	75
Cumple parcialmente	20
No aplica	16
Cumple satisfactoriamente	3
Total general	**114**

OBSS

Dirección	Cargo
Dirección de Redes	Gerente General
Responsable Técnico	Líder Técnico
Dirección de Redes	Arquitecto de Redes

Dirección de Redes	Técnico de Redes
Dirección de Seguridad.	Oficial de Seguridad

Dirección de Seguridad.	Profesional de Seguridad.
Dirección de TI	Técnico de soporte

Dirección Comercial	Ejecutivo Comercial Senior.
Dirección Financiera	Contador.
Dirección de RRHH	Bussines Parner

MATRIZ DE ROLES Y RESPO

Autoridad
Aprobar los documentos y planes para SGSI. Aprobación y adopción del SGSI. Asegurar que se realicen las acciones (preventivas, Correctivas, Mejora) cuando sea neceario. Aprobar documentos financieros e indicadores financieros de la empresa. Aprobar proyectos de alto impacto.
Aprobar la oferta técnico económica para presentar a cliente final. Aprobar los Flujos de implementación de las etapas contractuales. Asegurar que se implemente el SGSI acorde a necesidad. Aprobar los informes y pruebas realizadas en la implementación de proyecto. Asegurar que se lleven acabo los comités de inicio de proyecto.
Asignar actividades de diseño a los técnicos de redes. Aprobar los diseños técnicos de diseño. Aprobar los flujos de trabajo junto con el Líder Técnico. Asegurar negociaciones con fabricantes o Terceros.

Asegurar los activos lleguen a los destinos de instalación de proyecto.

Asegurar las certificaciones técnicas de fabricantes.

Asegurar cumplimiento de cronograma con equipos de cuadrillas asociadas a proyecto.

Apoyar en los comités internos de ingeniería.

Aprobar el recibido de la infraestructura contratada.

Aprobar los documentos de inventarios de infraestructura.

Aprobar la documentación requerida para el diseño y posterior implementación del SGSI para OBSS.

Aprobar el plan de adopción y capacitación del SGSI.

Aprobar las características técnicas de los activos que adquiera OBSS a nivel de Seguridad.

Asegurar personal de apoyo para la adopción del SGSI.

Asegurar con los proveedores las capacitaciones de cultura del SGSI para OBSS.

Mantener la seguridad y la confidencialidad sobre la emisión y mantenimiento de la identificación de usuarios y contraseñas

Guiar al cuerpo directivo y a la administración de la organización ante incidentes de seguridad mediante un Plan de Respuesta a Incidentes, con el fin de atender rápidamente este tipo de eventualidades.

Asegurar los indicadores permanentes de seguridad de la información de OBSS. Solicitar al Oficial de Seguridad el acompañamiento en las recomendaciones de ciberseguridad, capacitación o concientización al interior de OBSS. Revisar con el Oficial de seguridad el cronograma de implementación de la SGSI. Identificar los riesgos de los activos de seguridad de OBSS. Disponer de la información para asegurar el SGSI. Aprobar las solicitudes de los usuarios para los accesos de información de la empresa OBSS. Definir e implementar políticas de seguridad acorde a las necesidades del cliente en cada proyecto en entornos de sistemas complejos y multi fabricante
Identificar los requerimientos de los usuarios respecto a las instalaciones de software. Autorizar la creación de nuevas cuentas bajo el dominio de la empresa OBSS. Solicitar a los fabricantes las garantías de los equipos. Mantener al día los documentos de recibido a satisfacción de los usuarios. Fomentar estrategias del buen alistamiento de los equipos cumpliendo con la norma SGSI.

Asginar la oportunidad al arquitecto de Redes. Identificar las necesidades del cliente y solicitar que se cumpla con lo requerido. Aprobar la oferta técnico económica desde el área comercial. Asegurar los ingresos de OBSS.
Aprobar el capex requerido por la unidad de Redes de OBSS. Asegurar el cumplimiento de los trámites contables y tributarios requeridos normativamente así como las respuestas requeridas por las autoridades y organismos de control.
Asegurar que los empleados cumplan con los manuales de la empresa OBSS. Promoveer el buen uso de las herramientas de la compañía. Aprobar encuentas de clima de la empresa OBSS. Asegurar la documentación de los empleados de OBSS. Apoyar la cultura Organizacional.

ONSABILIDADES

Responsabilidades
Procurar la disponibilidad de recursos para la implementación de proyectos. Monitorear que se este cumpliendo los indicadores financieros de la emrpesa. Vigilar que los requisitos del cliente se determinen y se cumplan Proporcionar los recursos necesarios para garantizar la implementación de los proyectos. Diseñar los planes de trabajo y la estrategia para lograr cierres efectivos. Fijar los Objetivos de Crecimiento de la compañía.
Acompañar y apoyar por el cumplimiento del SGSI. Lograr certificaciones para equipo de trabajo técnico de la empresa. Proporcionar apoyo de diseño de ingeniería para los proyectos nuevos. Fijar los objetivos de su equipo de trabajo.
Entender en detalle los requerimientos del cliente. Diseñar, preparar y sustentar los diseños del proyecto. Docuementar los casos de éxitos de implementación de proyectos. Realizar Cotización con los fabricantes o proveedores de la infraestructura adquirir para los proyectos. Apoyar en la implementación de los proyectos de ingeniería. Gestionar a los equipos involucrados.

Asistir a los programas de Entrenamientos y capacitación suministrado por la empresa OBSS.

Participar activamente en los Comités internos de mejora de los procesos de OBSS.

Ejecutar los proyectos definidos, cumpliendo con el alcance definido por el área de Redes de OBSS, diseño de Arquitectura.

Administrar la implementación, funcionamiento, actualización y mantenimiento preventivo y correctivo de la infraestructura de cada uno de los NODOS de la empresa OBSS.

Realizar Diagnostico de las necesidades de hardware y software para la empresa OBSS.

Documentar correctamente las instalaciones realizadas.

Asegurar la entrega del servicio en nivel de satisfacción alto.

Identificar el Modelo de seguridad y privacidad de la información y la situación actual de OBSS.

Diseñar el cronograma de la implementación del Modelo de SGSI.

Planear el plan de trabajo cumpliendo con los objetivos especificos del cronograma de proyecto de implementación de SGSI.

Gestionar el equipo de proyecto de la entidad, definiendo roles, responsabilidades, entregables y tiempos

Liderar la programación de reuniones de seguimiento y velar por la actualización de los indicadores de gestión del proyecto.

construir y afinar la documentación que garantice la correcta implementación y certificación futura de la norma ISO27001

Probar la arquitectura de seguridad para evaluar la fortaleza de la seguridad y para detectar las posibles amenazas

Mantener las reglas de acceso a los datos y otros recursos de TI

Entregar toda la información necesaria al Oficial de Seguridad para asegurar la correcta implementación del SGSI.

Garantizar la seguridad de la información y la ciberseguridad los proyectos actuales y nuevos de OBSS.

Organizar y preparar la información para facilitar al oficial de seguridad las actividades, avances y logros de las oportunidades de mejora respecto al SGSI y ciberseguridad de OBSS.

Fijar las acciones correctivas de los hallazgos de auditoría y los resultado de los procesos para asegurar el cumplimiento de la norma SGSI y mitigar los riesgos de la seguridad de la información de OBSS.

Realizar la medición de indicadores permanentes de seguridad de la información

Revisar configuraciones de seguridad perimetral de clientes, siendo capaz de identificar problemas y solucionarlos proactivamente

Instalar y configurar correctamente los SO, programas, Antivirus, aplicaciones y programas a ser empleada en la empresa OBSS.

Realizar atención de usuario en primer nivel en atención de falla de los equipos.

Configurar el equipo con los altos standares de cumplimiento de la seguridad de la información.

Asistir a las capacitaciones sobre las nuevas tendencias de ciberdelincuencia y como actuar.

Evaluar y garantizar que las nuevas aplicaciones funcionen correctamente antes de su implementación en los sistemas.

Llevar acabo revisiones de seguridad en todos los sistemas

Tener un buen relacionamiento comercial con los clientes. Realizar presentación de la oferta técnico Económica. Responsable de el seguimiento y necesidades del cliente. Generar nuevas ventas y reclutar nuevas oportunidades. Responsable de la facturación sobre la cartera de clientes asignadas.
Apoyar la gestión de los procesos de contabilidad, tesorería y pagos, legalizaciones y monitoreo de cartera. Estructurar el plan financiero y el presupuesto de los proyectos, ejecutar y monitorear las acciones para su desarrollo, asegurando el cumplimiento a la estrategia financiera y corporativa de cada proyecto y convenio.
Capacitar a los empleados sobre las necesidades de desarrollo, el crecimiento profesional y las oportunidades de aprendizaje. Diseñar y facilitar programas de capacitación relacionados con recursos humanos para los empleados. Producir métricas e informes precisos y relevantes Llevar a cabo proyectos especiales según lo asignado

Clasificación del Activo	Activo de información
HARDWARE	Router de Borde
	Router distribución
	Router agregacion
	Servidor (radius y DNS)
	Computadores
	SW distribución POE
	Radio MIMOSA B11 (backhault)
	Radio MIMOSA B5C
	Radio CAMBIUM PTP 550E
	Radio MIMOSA C5C
	antenas Sectoriales
SOFTWARE	Sistema de monitoreo (API- telegram)
	Ofimatica (servidor)
	Correo (como Hosting)
	Documentos en Drive
	Software para línea de vista - Mikrotic - Cambium
REDES	WAN
	LAN
	Enlaces 2GB (banda milimetrica 60 y 80 Ghz)
	Rack
	Enlaces 1GB (banda licenciada 11 Ghz)
LUGAR	Predios
PERSONAL	Gerencia administrativa
	Ejectivo comercial senior
	Ejectivo comercial junior
	Revisor fiscal
	Contador
	Arquitecto redes
	Jefe tecnico
	Tecnicos de redes

Clasificación del Activo	Activo de Información	Ca Vulnerabilidades
HARDWARE	**Equipo Router Borde Router distribución Router agregacion**	No contar con licenciamiento de Seguridad y Cifrado
		No contar con el soporte de fabricante
		No Contar con Herramienta de Monitoreo
		Desactualización del Firware.
	Computadores	Software Maliciosos
		Virus informaticos
		Desconocimiento de los funcionarios para detectar casos que comprometan la seguridad de la información.
		Gestión de Contraseñas
		No definir correctamente los privilegios o permisos.
		Puertos de USB no bloqueados.
	Servidor DNS	Vulnerabilidad DNS
		Vulnenrabilidad de ataques de Usurpación
		Vulenrabilidad en ataques Cbeneticos

		Vulenrablidad en el Commmand And Control
	SW distribución POE	falla de inyección de comandos
		omisión de autenticación
		*Vulnerabilidad que permite la divulgación de información
		*vulnerabilidad de solicitudes de validación en la interfaz de usuario web
LUGAR	**Predios**	No contar con sistemas de CCTV.
		Fenómenos Ambientales.
REDES	**Racks**	Corrosión de Humedad
		Puerta del RACK sin Seguro
		Cableado no Organizado(peinado)
SOFTWARE	**Docuemntos Ondrive**	Acceso a los archivos compartidos en el OneDrive.
		Secuestro de cuentas por usuario.
		Claves no seguras

ausas Amenzas	Impacto
Acceso por parte de terceros a los equipos enrutadores.	Ataques a la servicios de la empresa.
No disponer atención a Fallas nivel 3	Servicios no funcional y de garantías de partes del equipo.
No tener control del estado del servicio.	Disponibilidad mayor del Servicio, multas por incumplimientos de ANS.
Los ciberatacantes puede acceder al router si no se cuenta con actualizaciones correspondientes sobre el router.	Acceder a la red, generando Indisponibnilidad.
Ataques Informaticos	Secuestro y pérdida de Información.
Infección de Archivos.	Daño de Arquivos que comprometan información confidencial de la empresa. Keyloggers se instalan por medio de los troyanos y roban datos de accesos a sitios WEB, sitios bancarios y cuentas personales.
Amenazas de Phising	Robo de información personal y de la empresa.
Amenazas de peticiones de acceso.	Realización de fuerza brua para acceder a la bases de datos, sistemas operativos etc
Contraseñas inseguras,limitar incorrectamente el acceso a plataformas o archivos que no sean parte de la funcion o roles que competen de los funcionarios.	Acceso a información confidenacial de la organización, daño de archivos por desconocimiento.
Extracción de información vulnerable. Infección de Virus.	Exponer información confidencial de la empresa para uso mal intencionado. Daño de archivos confidenciales de la empresas.
Consulta a Sitios incorrectos	una mala asignación en la busqueda genrando retrasos
amenaza en la utilización de dominios similares	Se presta paraque el DS sea atacado por usurpación de dominio,.
Engaño al usuario para que acceda a sitios no seguros	EL DNS puede estar afectado por ataques de PHISING

Ataques Cibeneticos por medio de Malware	EL DNS se puede aprovechar para ataques de Malware.
*Ataques ciberneticos	*permite escalas de privilegios; para ser explotada, los atacantes requieren un inicio de sesión legítimo para acceder a la interfaz web del switch.
*Cargue masivo de archivos	*los hackers cargar archivos arbitrarios en el dispositivo *ataque de DoS
*Divulgación de información del cliente.	*Se debe a la falta de validación de seguridad con controles de autenticación para acceder a la interfaz de usuario web.
	* atacante podría aprovechar esta vulnerabilidad de seguridad para enviar una solicitud HTTP maliciosa a la interfaz de usuario
Robo de la infraestuctura, Invasión del terreno.	Caida de los servicios a usuario final
Incendios, Deslizamientos de Tierra, Inundaciones	Caida de los servicios y la no recuperación de los activos. Perdital total de los activos de la Estación base
Daño de la infraestructura alojada o instalada.	Daño de los equipos activos.
Acceso directo a los equipos activos.	Afectación del Servicio y corte de cableado estructurado.
Confusión de los cables de cada equipo	Afectación en cumplimiento a los tiempos de ANS en arreglar un servicio.
Extracción de la información o eliminación de la información.	Confidencialidad, Disponibilidad e Integridad de la información.
perdida de la información	Robo de información personal y de la empresa.
Acceso a la información de la empresa.	Hackeo de la infomación confidencial.

Probabilidad de Ocurrencia	Consecuencia de La Ocurrencia
Muy Alta	Mayor
Media	Moderada
Muy Alta	Mayor
Alta	Mayor
Alta	Mayor
Muy Alta	Máxima
Muy Alta	Mayor
Muy Alta	Mayor
Alta	Mayor
Muy Alta	Mayor
Alta	Mayor
Media	Mayor
Alta	Mayor

Muy Alta	Máxima
Alta	Mayor
Alta	Mayor
Alta	Mayor
Alta	Mayor
Alta	Mayor
Alta	Moderada
Alta	Mayor
Alta	Mayor
Alta	Mayor
Muy Alta	Mayor
Muy Alta	Mayor
Muy Alta	Mayor

IMPACTO	
Confidencialidad	**Integridad**
Alta	Alta
Media	Alta
Baja	Baja
Muy Alta	Muy Alta
Muy Alta	Muy Alta
Muy Alta	Alta
Muy Alta	Muy Alta
Muy Alta	Alta
Muy Alta	Media
Media	Alta
Media	Alta
Media	Alta
Media	Alta

Media	Alta
Media	Alta
Media	Alta
Media	Alta
Media	Alta
Media	Alta
Media	Media
Baja	Alta
Baja	Baja
Baja	Baja
Alta	Alta
Alta	Alta
Alta	Alta

Disponibilidad	Valor del Impacto	Nivel del Impacto
Muy Alta	**40**	Riesgo Extremo
Alta	**12**	Riesgo Tolerable
Alta	**40**	Riesgo Extremo
Muy Alta	**32**	Riesgo Extremo
Muy Alta	**32**	Riesgo Extremo
Media	**80**	Riesgo Extremo
Alta	**40**	Riesgo Extremo
Media	**40**	Riesgo Extremo
Alta	**32**	Riesgo Extremo
Alta	**32**	Riesgo Extremo
Alta	32	Riesgo Extremo
Alta	24	Riesgo Alto
Alta	32	Riesgo Extremo

Alta	80	Riesgo Extremo
Alta	32	Riesgo Extremo
Alta	32	Riesgo Extremo
Alta	32	Riesgo Extremo
Alta	32	Riesgo Extremo
Alta	32	Riesgo Extremo
Media	16	Riesgo Alto
Muy Alta	32	Riesgo Extremo
Muy Alta	32	Riesgo Extremo
Muy Alta	32	Riesgo Extremo
Alta	40	Riesgo Extremo
Alta	40	Riesgo Extremo
Alta	40	Riesgo Extremo

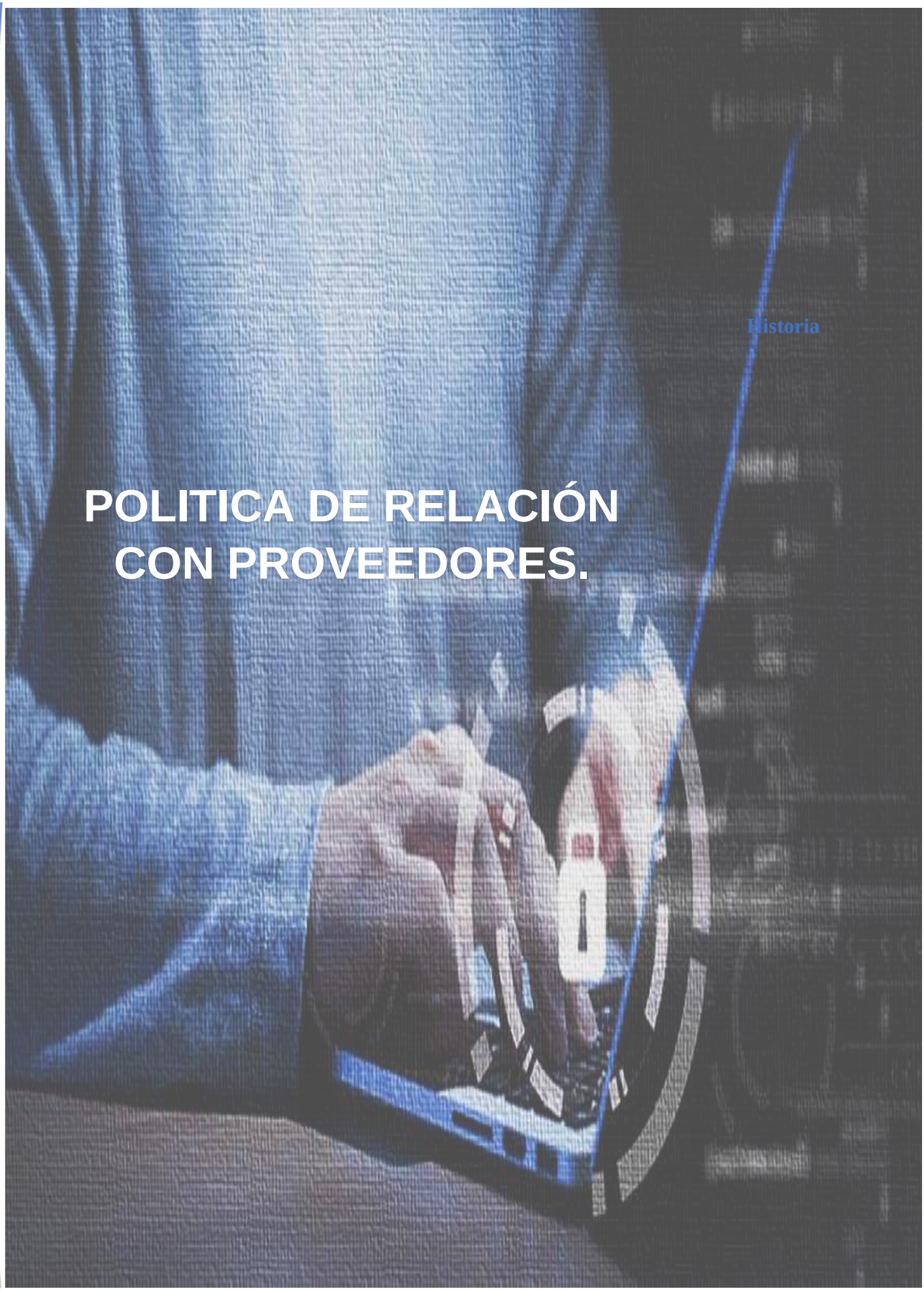
		MATRIZ DE IMPACTO				
		CONSECUENCIA				
		Mínima	Menor	Moderada	Mayor	Máxima
PROBABILIDAD		1	2	4	8	16
Muy Alta	5	5	10	20	40	80
Alta	4	4	8	16	32	64
Media	3	3	6	12	24	48
Baja	2	2	4	8	16	32
Muy Baja	1	1	2	4	8	16

NIVEL DEL IMPACTO
Riesgo Aceptable
Riesgo Tolerable
Riesgo Alto
Riesgo Extremo

COLOR	Valor del Activo	Clasificación
	Muy Alta	5
	Alta	4
	Media	3
	Baja	2
	Muy Baja	1

https://www1.elvatron.com/equipos-de-puesta-a-tierra-y-aislamiento/7-consecuencias-de-un-mal-s
https://repository.unad.edu.co/bitstream/handle/10596/17396/18520719.pdf?sequence=1&isAllov
https://securelist.lat/vulnerabilidades-en-antenas-de-comunicacion-satelital-podrian-convertirlas-er
https://repository.unad.edu.co/bitstream/handle/10596/28221/93405573.pdf?sequence=1&isAllov
https://biblioteca.uoc.edu/es/actualidad/noticia/Las-principales-amenazas-de-los-archivos-digitales.
https://evaluandocloud.com/amenazas-seguridad-almacenamiento-datos-la-nube/

ı-armas-que-atacan-con-campos-de-radiacion-de-alta-intensidad/87490/



Historia

POLITICA DE RELACIÓN CON PROVEEDORES.

HISTORIA

Versión	Fecha	Cambios Introducidos
1.0.0	**12/10/2022**	**Versión Inicial del Documento.**

TABLA DE CONTENIDOS

1. ANTECEDENTES

OBSS INGENIERÍA es una empresa del sector de las telecomunicaciones y como objeto principal de su actividad es la prestación de servicios de Internet por medio de radioenlaces, es importante tener establecido una política de relación con proveedor, dado que necesita la contratación de servicios especializados externos que permiten de una u otra forma soportar su actividad. Para ello es importante no solo definir o asegurar que los sistemas de OBSS INGENIERÍA estén protegidos, si no que se debe tener la misma exigencia de seguridad a los proveedores externos que gestionan parte de la información que se considera sensible y puede vulnerar la seguridad a la empresa OBSS INGENIERÍA.

Entre los proveedores se destacan los siguientes grupos:

- **Proveedores de servicios tecnológicos.** Son Aquellos proveedores que ofrecen servicios web y de soporte informático, proveedores de servicios en la nube.
- **Proveedores de Servicios No Tecnológicos.** Son aquellos proveedores que prestan servicios financieros, viajes, publicidad, marketing.
- **Suministradores de productos tecnológicos.** Estos proveedores son aquellos que prestan equipos de tecnología(hardware), aplicaciones informáticas etc.

2. OBJETIVO

El objetivo de esta política de gestión de proveedores se trata de controlar toda la relación que se pueda llevar a cabo con cualquier tipo de proveedor y en particular cuando estos tienen acceso a parte o toda la información de la empresa. Para ello es importante establecer contratos y acuerdos que aseguren como se debe contemplar la protección de la seguridad antes, durante y al finalizar cualquier tipo de servicio. Además de ello OBSS INGENIERÍA debe asegurar que cualquier tipo de producto o servicio contratado debe cumplir con los requisitos de seguridad establecido por la empresa.

3. CHECK LIST

Para dar cumplimiento a la política de seguridad en relación con proveedores, a continuación, se incluyen unos controles que pueden clasificarse en dos niveles. [1]

- **CONTROL BÁSICO:** Es el esfuerzo necesario para que se aplique por medio de funcionalidades sencillas y que sean asumibles. Se previene ataques mediante la instalación de herramientas de seguridad elementales.

- **CONTROL AVANZADO:** Es el esfuerzo necesario para que se aplique por medio de funcionalidades complejas. Se previene ataques mediante la instalación de programas robustos. Se puede usar mecanismos de recuperación ante fallos.

Los controles podrán tener el siguiente alcance:

- PROCESOS: aplica para la dirección de OBSS INGENIERÍA o Personal de gestión.
- TECNOLOGÍA: aplica para personal técnico especializado.
- PERSONAS: aplica a todo el personal de OBSS INGENIERÍA.

[1] https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/relacion-proveedores.pdf

NIVEL	ALCANCE	CONTROL
BÁSICO	PROCESOS	**Requisitos mínimos cumplibles de seguridad en productos y servicios** OBSS INGENIERÍA establecerá cuáles serán los requisitos de seguridad mínimos que debe cumplir los proveedores y/o terceros respecto a los productos que adquiere la empresa y los servicios que contrata.
AVANZADO	PROCESOS	**Definir cláusulas contractuales en materia de seguridad de la información** Eres riguroso en la elaboración y aceptación de las cláusulas contractuales en materia de ciberseguridad.
AVANZADA	TÉCNOLOGÍA	**Definir las responsabilidades concretas entre OBSS INGENIERÍA Y el proveedor, contratista, Tercero etc.** Delimitas las responsabilidades en materia de ciberseguridad para cada una de las partes involucradas
BÁSICO	PROCESOS	**Definir los ANS (Acuerdos de Nivel de Servicio)** Se definirá cuáles serán los ANS que acepta OBSS INGENIERÍA al momento de contratar cualquier servicio.
BÁSICO	PROCESOS	**Controles de seguridad obligatorio que debe cumplir los proveedores con OBSS INGENIERÍA.** Determinar que controles de seguridad son de obligatorio cumplimiento en las relaciones con los proveedores de servicios tecnológicos.
BÁSICO	PROCESOS	**Certificación de los Servicios contratados por OBSS INGENIERÍA** Exigir a los proveedores las certificaciones que den garantía a la calidad de los servicios y que se encuentran con políticas de seguridad.
BÁSICO	PROCESOS	**Auditoría y control de los servicios contratados por OBSS INGENIERÍA.** Supervisar que los productos y servicios contratados responden a lo acordado en materia de ciberseguridad.
BÁSICO	PROCESOS	**Finalización de la relación contractual** Garantizar la seguridad de la información tras la finalización de un servicio o contrato.

Tabla 1Clasificación de Controles para con los proveedores. ***(Relación con proveedores, 2020)***

4. PUNTOS CLAVE DE LA POLÍTICA.

Los puntos clave para que la política tenga la mejor adopción en la empresa OBSS NGENIERÍA corresponden a:

- **Requisitos de seguridad en productos y servicios**: OBSS INGENIERÍA deberá definir cuales son los requisitos en ciberseguridad que debe cumplir los proveedores al momento de adquirir cualquier servicio, es importante nuevamente aclarar que OBSS INGENIERÍA es prestadora de servicios de internet por medio de Radio enlaces, por lo que con mayor precisión este requisito debe regirse en estricto cumplimiento con las políticas de seguridad de la información de OBSS INGENIERÍA y de igual forma se deberá extender a los proveedores, colaboradores etc. (Relación con proveedores, 2020)

- **Definir cláusulas contractuales en materia de seguridad de la información**: Con cada uno de los proveedores con los que OBSS INGENIERÍA establezca alguna relación contractual, se deberá definir acuerdos rigurosos en materia de ciberseguridad y premisas de confidencialidad de la información.

  También se debe definir como se accede a la información, como puede llegar hacer accedida y como se clasificará y protegerá. También OBSS INGENIERÍA debe asegurar que, una vez finalizado el contrato con el proveedor de servicios, no podrá acceder o mantener cualquier información que sea sensible para OBSS INGENIERÍA.

- **Definir las responsabilidades concretas por ambas partes.** OBSS INGENIERÍA, establecerá por contrato penalizaciones, cumplimientos de Acuerdos de niveles de Servicios (ANS), si es el proveedor o la empresa la que es responsable de cualquier aspecto relativo o ligado a la seguridad de la información, para ello se debe controlar que personas acceden a la información sensible.

5. GESTIÓN DE LA PRESTACIÓN DEL SERVICIO POR SUMINISTRADORES.

El objetivo es establecer acuerdos en el nivel de seguridad indicado y mantener una relación con los proveedores y que estén alineados con los siguientes acuerdos:

(https://www.iso27000.es/iso27002_15.html, 2022)

5.1 RIESGOS ASOCIADOS

- OBSS INGENIERÍA debe verificar que la implementación de los servicios debe ir acompañada de un monitoreo de cumplimiento y gestión de cambios dado que así asegura que los servicios contratados están cumpliendo con los requerimientos solicitados entre OBSS INGENIERÍA Y EL TERCERO.

- Es importante que OBSS INGENIERÍA valide que los servicios contratados cumplen con lo solicitado, por lo que es importante asegurar una supervisión de contratos y servicios con los proveedores y así mismo asegurar que a la entrega cumpla con el 100% de satisfacción de entrega.
- OBSS INGENIERÍA debe validar de manera periódica los acuerdos de niveles de servicios establecidos en el contrato con el tercero, ya que algunas veces no están bien detallados y pueden ser casos de sistemas de castigo para OBSS INGENIERÍA.

5.2 RIESGOS ASOCIADOS

- **Supervisión y revisión de los servicios prestados por terceros:** OBSS INGENIERÍA debe monitorear, revisar y tener un control de auditoría para la presentación de servicios contratados con el proveedor.
- **Gestión de cambios en los servicios prestados por terceros:** Se deberían administrar los cambios a la provisión de servicios que realizan los proveedores manteniendo y mejorando:
- las políticas de seguridad de la información
- los procedimientos y controles específicos.
- Se debería considerar la criticidad de la información comercial, los sistemas y procesos involucrados en el proceso de reevaluación de riesgos. (https://www.iso27000.es/iso27002_15.html, 2022)

Bibliografía

https://www.iso27000.es/iso27002_15.html. (01 de 04 de 2022). *ISO 27001 ES.* Obtenido de ISO 27001 ES: https://www.iso27000.es/iso27002_15.html

Relación con proveedores. (21 de 05 de 2020). Obtenido de Relación con proveedores: https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/relacion-proveedores.pdf

Política de gestión de incidentes OBSS

Contenido

1. Introducción

La política de gestión de incidentes tiene como finalidad definir la directriz para la atención de incidentes de acuerdo con su clasificación de criticidad. Para es necesario establecer los ANS de atención, los roles que ejecutaran el plan de acción y proceso que se debe seguir para lograr el menor impacto a la organización.

La gestión de los acuerdos de nivel de servicio - ANS - o SLA (Service Level Agreement Management), es el proceso que se encarga de definir, documentar, acordar, monitorear, medir, reportar y revisar el nivel de los servicios que provee OBSS.

2. Objetivos

El objetivo principal de la gestión de incidentes es definir el marco de acción frente a los posibles escenarios de fallas de los sistemas de información con los que cuenta la organización OBSS y puedan llegar a afectar a los servicios propios o en el ejercicio mismo de proveer servicios de internet para múltiples clientes.

2.1 Objetivos específicos

- Definir los lineamientos que se deben seguir en caso de presentarse un incidente.
- Definir el nivel de criticidad de un incidente que se pueda presentar en los servicios de la organización.
- Definir los ANS para la prestación de los servicios.
- Establecer los roles que participaran en la resolución de fallas.

3. Gestión de incidentes

Un incidente es un evento que afecta la disponibilidad, integridad o confidencialidad de la información de la infraestructura tecnológica de la Entidad, por lo cual a continuación se relacionan los tiempos de atención y solución por parte de los recursos asociados al servicio, que administran la infraestructura, plataformas y demás componentes que hacen parte de la solución, teniendo como base la definición de los niveles de atención.

3.1 Definición de los Niveles de Atención

En la siguiente tabla, se describe el impacto del incidente, teniendo como base la definición del criterio de la falla que se pueda presentar:

CLASIFICACION DE INCIDENTES	
PRIORIDAD	**DESCRIPCION**
Significativo	Un incidente de prioridad alta, que causa una falla en la infraestructura o plataforma de la organización. Es comportamiento no habitual que causa perdida severa de los servicios o la solución. La operación podría verse suspendida o restringida.
Moderado	Un incidente de prioridad media puede causar una perdida mínima en la infraestructura o plataforma de la organización. Es un inconveniente de menor impacto que se puede remediar de forma parcial o provisional y dar continuidad a las actividades.
Menor	Un incidente de prioridad baja, no causa perdida ni afectación del servicio o infraestructura, es una falla que no limita la ejecución de las actividades

3.2 Tiempos de atención

A continuación, se definen los tiempos de atención óptimos para la atención de fallas de acuerdo con la clasificación de criticidad:

Tipo de Incidente	Descripción del Incidente	Tiempo de Respuesta
Significativo	El servicio completo está afectado.	2 horas
Moderado	El servicio está afectado en forma intermitente	8 horas
Menor	Una condición de error intermitente que no afecta el servicio	24 horas

3.2 Niveles de atención

3.2.1 Soporte Primer Nivel de Atención

Se concibe un soporte de Primer Nivel de atención (líder técnico OBSS), qué a través de los canales de atención como telefónico, buzón de correo y herramienta de gestión web, brindará atención y gestión ante incidentes, requerimientos y consultas de los servicios ofertados, realizará el registro, categorización, priorización, pruebas y descartes de primer nivel, para dar solución, de lo contrario realizará escalamiento al equipo especializado de soporte de la operación de nivel 2.

3.2.2 Soporte segundo Nivel de Atención

Del mismo modo, se contempla un equipo especializado de operación y soporte de los servicios de Conectividad, Seguridad y Redes, quienes tienen como objetivo primordial la gestión y soporte de los servicios, atendiendo los casos reportados y escalados por el primer nivel; este equipo especializado realizará el diagnosticando y análisis de la causa raíz y determinar la posible solución parcial o definitiva a incidentes, requerimientos y problemas que se presenten sobre los servicios.

3.2.3 Soporte tercer Nivel de Atención

Se contempla el Tercer Nivel a través de proveedores y fabricantes, los cuales se integrarán a la operación del servicio, brindando apoyo especializado, a través del escalamiento directo a nivel de soporte, mantenimiento, gestión de garantías y suministro de partes y equipos.

Cuando la solución requiera desplazamiento a sitio los tiempos de atención serán los siguientes:

Soporte	Ingeniero en Sitio
Ciudades Principales	5 horas
Ciudades Intermedias	12 horas
Ciudades y Municipios Remotos	24 horas

A continuación, se definen los roles de los cuales dispone OBSS para los niveles de atención:

Niveles de atención	Rol
Nivel 1	Técnico de Redes
Nivel 2	Profesional de Seguridad Arquitecto de Redes
Nivel 3	Fabricantes Técnico de soporte

4. Aceptación

Elaborado por	Cargo	Fecha
Harold Fabian Chilatra	Especialista de seguridad	30/10/2022
Leidy Cubillos Poveda	Especialista de seguridad	30/10/2022
William Hernandez Leal	Líder técnico OBSS	30/10/2022

Historia

PLAN DE CONTINUIDAD DEL NEGOCIO

HISTORIA

Versión	Fecha	Cambios Introducidos
1.0.0	**02/11/2022**	**Versión Inicial del Documento.**

TABLA DE CONTENIDOS

1. INTRODUCCIÓN

Para OBSS INGENIERÍA es importante partir con el diseño de un SGSI (Sistema de Seguridad de la Información), ya que esto exige que se tenga también dentro del diseño del SGSI basado en la norma ISO 27001:2013, un proceso que preserve la información ante situaciones vulnerables como los desastres, las fallas que se puedan llegar a presentar, la perdida de cualquier servicio dentro de OBSS INGENIERÍA e incluso la disponibilidad del servicio. Por ello es importante asegurar dentro del diseño a suministrar a la empresa OBSS INGENIERÍA un proceso conocido como la gestión de continuidad del negocio. Cuando se lleva a cabo una buena implementación de la gestión de continuidad del negocio, se puede prever la disminución de ocurrencia de incidentes disruptivos; y en caso de que estos se llegarán a presentar la empresa OBSS INGENIERÍA, podrá estar en la capacidad de poder responder de manera adecuada y oportuna, por lo que garantiza que hay una reducción significativa del daño potencial que pueda ocasionar cualquier incidente para la empresa.

La gestión de continuidad de negocio, es la que se encarga de identificar cuales son los posibles impactos que pueden llegar amenazar las actividades de OBSS INGENIERÍA, y para ello es importante construir un plan de acción que permita la construcción de la resistencia y respuesta rápida y efectiva que garantice el mayor desarrollo de los procesos para que OBSS INGENIERÍA pueda dar cumplimiento a su misión y propósito organizacional, es decir lo que hace ser la naturaleza de la empresa que es el prestar los servicios de conectividad de radioenlaces para el departamento del Tolima. Para llevar a cabo una buena práctica de implementación del plan de continuidad de negocio para OBSS INGENIERÍA, se debe disponer de recurso humano, financiero, físico y tecnológico.

2. OBJETIVO DE LA PLAN DE CONTINUIDAD DEL NEGOCIO.

Fortalecer, Garantizar y consolidar cualquier capacidad de respuesta por parte de OBSS INGENIERÍA, ante eventos ya sean naturales, o de afectación de servicio, mediante la creación de un plan de continuidad que garantice el restablecimiento de la operación de los servicios afectados de OBSS INGENIERÍA.

3. GESTIÓN DE CONTINUIDAD DEL NEGOCIO

Como se puede observar en la ilustración 1, el modelo de operación de seguridad de la información, para el plan de gestión de continuidad se tendrán en cuenta las fases de planificación, implementación, gestión , mejora continua y diagnóstico, para OBSS INGENIERÍA , este modelo es perfecto dado que garantiza que desde el momento en que se lleven a cabo la implementación del SGSI y desde el diseño asegurará que la empresa pueda ejecutar planes que garanticen como entrar el servicio en el menor tiempo posible y como reaccionar ante este tipo de eventos.

Ilustración 1 Continuidad del Negocio_ FUENTE: MINTIC

OBSS INGENIERÍA será responsable de realizar la implementación y el desarrollo de los planes de continuidad a nivel interno, ya sea por plataformas propias de la empresa o dejarlas documentadas para con ello tener como objetivo la reanudación de la operación de los procesos de información de manera rápida y oportuna, sin afectar a gran escala los servicios de los clientes finales en caso de que suceda una situación de alto riesgo.

Desde el diseño del SGSI para OBSS INGENIERÍA, se dejan identificados el inventario de los activos, pero OBSS INGENIERÍA, será responsable de indicar que tan críticos son frente a la disponibilidad de los servicios.

Como se ha mencionado anteriormente el proceso de continuidad de Negocio identifica los impactos que son potenciales y que amenazan la continuidad de las actividades de la empresa, por ello es importante dejar un marco de referencia para OBSS INGENIERÍA, donde se de un plan de respuesta efectiva y que le permita brindar protección a los clientes y usuarios.

Este documento será un complemento de modelo de seguridad y privacidad de la información y constituye un referente de la continuidad del negocio para OBSS INGENIERÍA.

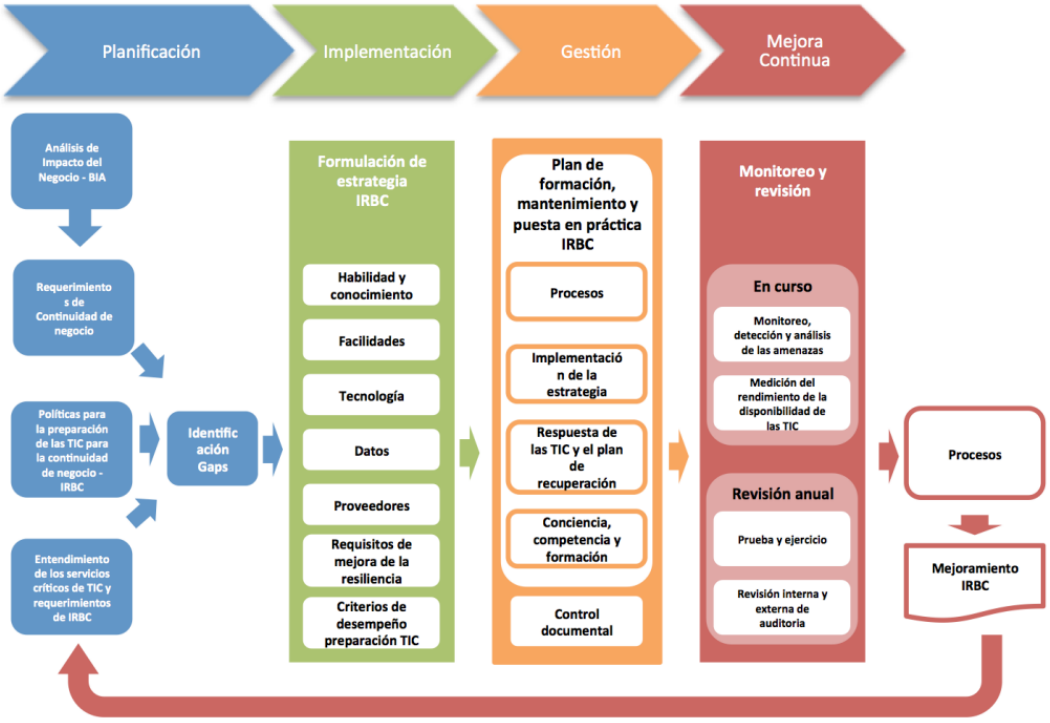


Ilustración 2 Marco Continuidad del Negocio para Seguridad y Privacidad de la Información FUENTE: MINTIC

Para OBSS INGENIERÍA en el diseño del SGSI que se entregará a la empresa, se hará referencia a programas de SGSI que permita mejorar la preparación de las empresas y se pueda permitir:

- Responder de manera cambiantes el ambiente de los riesgos.
- Asegurar la continuidad del negocio cuando haya afectación de operaciones críticas del negocio.
- OBSS INGENIERÍA deberá estar preparada para responder antes que cualquier evento pueda ocurrir, y poder identificar los eventos que pueden llegar a estar relacionados a incidentes.
- Responder y recuperarse de los incidentes.

A continuación, se detalla los componentes que OBSS INGENIERÍA debe tener en cuenta para garantizar la estrategia de establecimiento de los servicios.

1. PLANIFICACIÓN PARA LA PREPARACIÓN DE LAS TIC PARA LA CONTINUIDAD DEL NEGOCIO
2. IMPLEMENTACIÓN PARA LA PREPARACIÓN DE LAS TIC PARA LA CONTINUIDAD DEL NEGOCIO
3. EVALUACIÓN DE DESEMPEÑO PARA LAPREPARACIÓN DE LAS TIC PARA LA CONTINUIDAD DEL NEGOCIO
4. MEJORA CONTINUA PARA LA PREPARACIÓN DE LAS TIC PARA LA CONTINUIDAD DEL NEGOCIO

4. ANÁLISIS DEL IMPACTO DEL NEGOCIO.

El análisis del impacto del negocio permitirá a OBSS INGENIERÍA identificar con claridad cuales son los procesos importantes y como analizar el nivel de impacto con relación a la gestión de la continuidad del negocio. Para ello OBSS INGENIERÍA debe disponer de un documento que le permita identificar las áreas criticas del negocio y que este sea la base para que puedan hacer las respectivas mediciones del impacto, para ello es importante que se debe clarificar los siguientes requerimientos de cumplimiento: (MINISTERIO DE LAS TIC, 2010)

- Identificar las funciones y procesos importantes para la supervivencia de la entidad al momento de la interrupción, esto es tener en cuenta cuales de los procesos son claves para que entren en operación rápidamente asignándoles la mayor prioridad posible, frente a los de menor prioridad; debe quedar claro que para los procesos identificados como no tan prioritarios se deben preparar también planes de recuperación.

- Revisar las consecuencias tanto operacionales como financieras, que una interrupción tendrá en los procesos considerados de alta prioridad.

- Estimar los tiempos de recuperación, en razón a las posibles alteraciones de los procesos considerados de alta prioridad para el funcionamiento de las infraestructuras de TI.

El entregable de esta fase es un informe con el detalle de las funciones y procesos críticos del negocio. Este documento debe contener la información básica de los recursos requeridos y los tiempos de recuperación para que las entidades puedan poner en funcionamiento los servicios y por ende la continuidad del negocio. (MINISTERIO DE LAS TIC, 2010)

4.1 REQUERIMIENTOS DE TIEMPO DE RECUPERACIÓN.

Como parte del plan de continuidad del negocio de OBSS INGENIERÍA, es importante poder definir y entender los requerimientos de tiempo necesarios para recuperar los servicios que han sido interrumpidos por diferentes motivos dentro de OBSS INGENIERÍA; estos requerimientos obedecen a varios componentes que hacen referencia y concreta al tiempo disponible en la cual OBSS INGENIERÍA puede recuperarse oportuna y ordenadamente a las interrupciones en los servicios e infraestructuras de TI. Los componentes se describen a continuación:

MTD (Maximun Tolerable Downtime) o Tiempo Máximo de Inactividad

Tolerable. Espacio de tiempo durante el cual un proceso puede estar inoperante hasta que la empresa empiece a tener pérdidas y colapse.

RTO (Recovery Time Objective) o Tiempo de Recuperación Objetivo. Es el tiempo transcurrido entre una interrupción y la recuperación del servicio. Indica el tiempo disponible para recuperar sistemas y recursos interrumpidos.

RPO (Recovery Point Objective) o Punto de Recuperación Objetivo. Es el rango de tolerancia que la entidad puede tener sobre la pérdida de datos yel evento de desastre.

WRT (Work Recovery Time): Es el tiempo invertido en buscar datos perdidos y la realización de reparaciones. Se calcula como el tiempo entre la recuperación del sistema y la normalización de los procesos.**(MINISTERIO DE LAS TIC, 2010)**

4.2 METODOLOGÍA DE ANÁLISIS DE IMPACTO DEL NEGOCIO.

la metodología del Análisis de Impacto del Negocio consiste en definir una serie de pasos interactivos con el objeto de identificar claramente los impactos de las interrupciones y tomar decisiones respecto a aquellos procesos que se consideran críticos para la organización y que afectan directamente el negocio ante la ocurrencia de un desastre, estos pasos se muestran en esta ilustración:

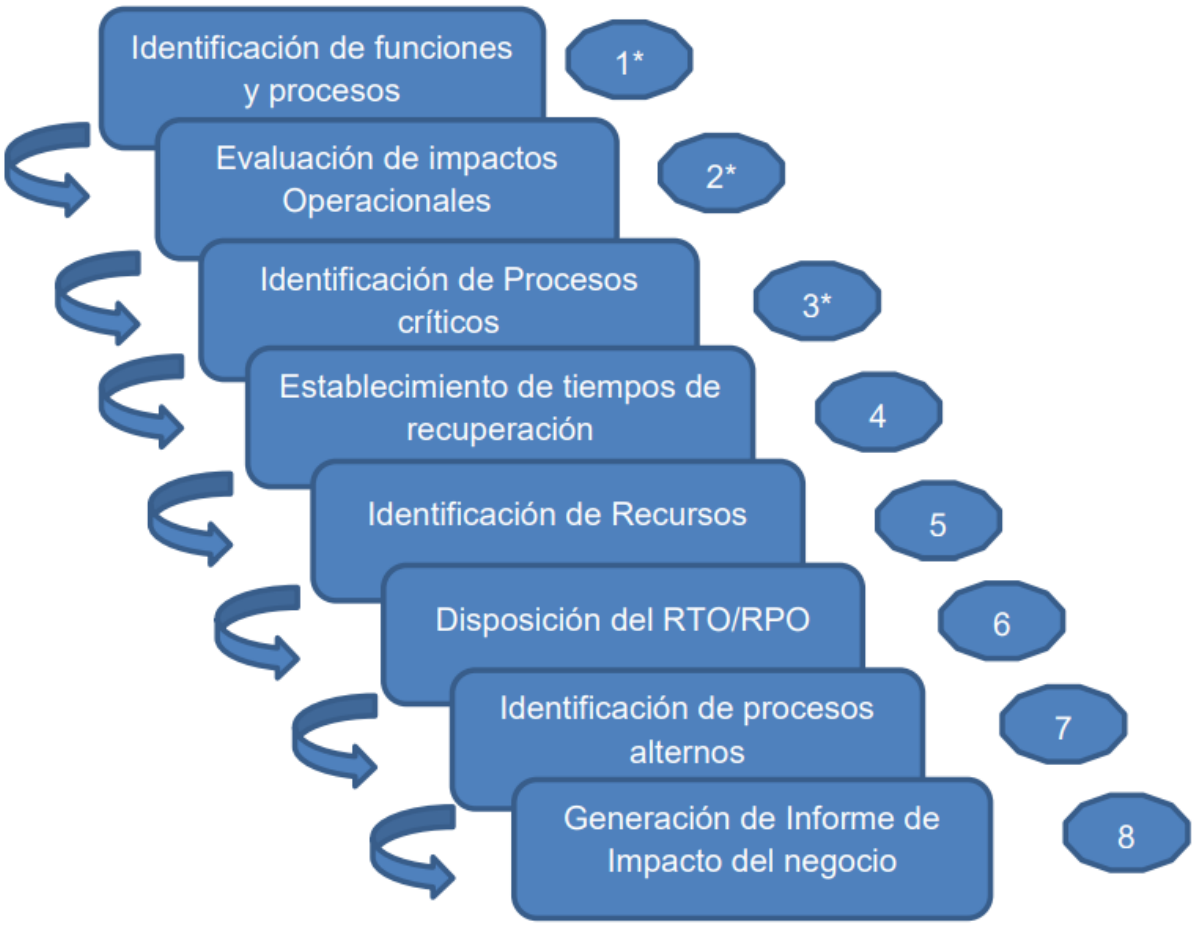


Ilustración 3 Metodología del Análisis de Impacto del Negocio FUENTE _ MINTIN

Bibliografía

MINISTERIO DE LAS TIC. (15 de 12 de 2010). *Guía para la preparación de las TIC*. Obtenido de Guía para la preparación de las TIC: https://www.mintic.gov.co/gestionti/615/articles-5482_G10_Continuidad_Negocio.pdf

No.	Tipo de norma	Título
1	Resolucion	Resolución 1075 de 2020
2	Resolucion	Resolución 1588 de 2012
3	Resolucion	Resolución 2118 de 2011
4	Resolucion	Resolución 917 de 2015
5	Resolucion	Resolución 83 de 2008 Ministerio de Comunicaciones
6	Resolucion	Resolución 970 de 2011
7	Decreto	Decreto 4392 del 23 de noviembre de 2010:
8	Decreto	Decreto 1161 de 2010 Nivel Nacional
9	Decreto	Decreto 4392 de 2010 Nivel Nacional
10	Decreto	Decreto 2044 de 2013 Nivel Nacional

11	Decreto	Decreto 542 de 2014 Nivel Nacional
12	Decreto	Decreto Único Reglamentario 1078 de 2015 Nivel Nacional
13	Decreto	Decreto 984 de 2022 Nivel Nacional
14	Ley	Ley 1341 de 2009 Nivel Nacional
15	Ley	Ley 1753 de 2015 Nivel Nacional
16	Ley	Ley 1978 de 2019 Congreso de la República de Colombia
17	Circular	Circular No. 01 de 2021
18	Norma	Norma ISO 27001
19	Norma	Norma ISO 27006
20	Norma	Norma ISO 27009

NORMAS QUE RIGEN LOS

Expedido por
MINTIC
MINTIC
MINTIC
MINTIC
MINTIC
MINTIC
MINTIC
MINTIC
MINTIC
MINTIC

MINTIC
MINTIC
MINTIC
MINTIC
MINTIC
MINTIC
MINTIC
ISO
ISO
ISO

PROCESOS , GESTIÓN, Y CONTROL DE EMPRESA OBSS

Síntesis o Aplicación específica
Por la cual se establecen las condiciones, requisitos y el trámite para otorgar o modificar permisos para el uso del espectro radioeléctrico, por el procedimiento de selección objetiva y se derogan las Resoluciones
Establece funciones del ministerio de las tecnologias de la informacion y las telecomunicaciones planear, asignar, gestionar y controlar el espectro radioelectrico, con el fin de fomentar la competencia, el pluralismo informativo, el acceso discriminatorio y evitar practicas monopolistas asi como mantener actualizado el cuadro nacinal de atribucion de bandas de frecuencias de Colombia con base en la necesidad del pais.
Constitución Política de Colombia en su artículo 75 dispone que “El espectro electromagnético es un bien público inenajenable e imprescriptible sujeto a la gestión y control del Estado”, por lo cual su uso debe
Por la cual se determinan las garantías para cubrir riesgos en materia de telecomunicaciones y de servicios postales.
Reglamenta la cesión de los permisos para el uso del espectro radioeléctrico conforme al marco normativo aplicable y con sujeción al Reglamento de Radiocomunicaciones de la Unión Internacional de Telecomunicaciones, UIT, y al Cuadro Nacional de Atribución de Bandas de Frecuencias. Señala el alcance de los permisos para el uso del espectro radioeléctrico, así como los requisitos para la solicitud de autorización de la cesión de permisos para su uso y las características de esta cesión.
se fijan los requisitos de tipo operativo para la obtención del título habilitante como Operador de Servicios Postales de Pago y se dictan otras disposiciones.
Por el cual se reglamenta la selección objetiva y la asignación directa por continuidad del servicio de que tratan los artículos 11 y 72 de la
Expide el régimen unificado de las contraprestaciones, el régimen sancionatorio y procedimientos administrativos asociados a las contraprestaciones en materia de telecomunicaciones de acuerdo con los artículos 13 y 36 de la Ley 1341 de 2009, con el fin de evitar la evasión y racionalizar los ingresos del Fondo de Tecnologías de la Información y las Comunicaciones, así como garantizar la igualdad en acceso a los distintos usuarios del espectro radioeléctrico.
Reglamenta la selección objetiva, así como el otorgamiento directo de permisos para uso temporal del espectro radioeléctrico por razones de continuidad del servicio, atendiendo, en todo caso, los principios orientadores de las actuaciones administrativas señaladas en el Código Contencioso Administrativo.
Establece los requisitos y las condiciones para la renovación de los permisos para el uso del espectro radioeléctrico catalogado por el Ministerio de Tecnologías de la Información y las Comunicaciones como IMT, de que trata el artículo 12 de la Ley 1341 de 2009, así como los requisitos para la renovación de los permisos bajo el régimen de transición previsto en el artículo 68 de dicha ley.

La norma reglamenta los artículos 10, 13 y 36 de la Ley 1341 de 2009 por medio de la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones TICs, y crea la Agencia Nacional de Espectro. El Decreto tiene por objeto fijar el alcance de los elementos que configuran la contraprestación periódica que deben pagar los proveedores de redes y de servicios de telecomunicaciones a favor del Fondo de Tecnologías de la Información y las Comunicaciones. Lo anterior, sin perjuicio de la aplicación del régimen de transición establecido en el artículo 68 de la misma ley y en el numeral 1 del artículo 58 de la Ley 1450 de 2011. Además establece los criterios para la determinación de las contraprestaciones económicas que se causan
Se establecen los requisitos y las condiciones para la renovación de los permisos para el uso del espectro radioeléctrico catalogado por el Ministerio de Tecnologías de la Información y las Comunicaciones como IMT, de que trata el artículo 12 de la Ley 1341 de 2009. así como los requisitos para la renovación de los permisos bajo el régimen de transición previsto en el artículo 68 de dicha ley. Ahora bien, Los Proveedores de Redes y Servicios de Telecomunicaciones (PRST) interesados en obtener la renovación de sus permisos para el uso del Espectro Radioeléctrico en los términos del artículo 12 de la Ley 1341 de 2009, deberán manifestar dicha intención con tres (3) meses de antelación a la fecha de vencimiento del título cuya renovación se solicita
Fija el tope máximo de espectro radioeléctrico por proveedor de Redes y Servicios de Telecomunicaciones para uso en servicios móviles terrestres (IMT), atendiendo recomendaciones de la Superintendencia de
Establece que el uso del espectro radioeléctrico requiere permiso previo, expreso y otorgado por el Ministerio de Tecnologías de la Información y las Comunicaciones. Precisa el plazo y renovación de los permisos para el uso del espectro radioeléctrico, la contraprestación económica por la utilización del mismo, las inhabilidades para acceder a los permisos de uso, crea el registro de la información relevante de redes, habilitaciones, autorizaciones y permisos.
Adopta el Plan Nacional de Desarrollo 2014-2018 "Todos por un nuevo país". La cesión de los permisos de uso del espectro radioeléctrico no generará contraprestación alguna a favor de la Nación. El negocio jurídico que, para este propósito, se celebre entre cedente y cesionario se sujetará al derecho privado, y a la aprobación del Ministerio de las TICS. (artículo 262).
Establece que el uso del espectro radioeléctrico requiere permiso previo, expreso y otorgado por el Ministerio de Tecnologías de la Información y las Comunicaciones. El permiso de uso del espectro respetará la neutralidad en la tecnología siempre y cuando esté coordinado con las políticas del Ministerio de Tecnologías de la Información y las Comunicaciones, no generen interferencias sobre otros servicios, sean compatibles con las tendencias internacionales del mercado, no afecten la seguridad nacional, y contribuyan
Aplicación de las disposiciones contenidas en la ley 679 de 2001 y el título 10 del decreto 1078 de 2015. cumplimiento de medidas destinadas a prevenir la difusión de contenidos ilegales con material de explotación, de pornografía y demás formas de abuso sexual en niñas, niños y adolescentes y el acceso de menores de edad a cualquier modalidad de información pornográfica a través de redes globales de
La ISO 27001:2013 es la norma internacional que proporciona un marco de trabajo para los sistemas de gestión de seguridad de la información (SGSI) con el fin de proporcionar confidencialidad, integridad y disponibilidad continuada de la información, así como cumplimiento legal.
ISO 27006 está pensada para apoyar la acreditación de organismos de certificación que ofrecen la certificación del Sistema de Gestión de Seguridad de la Información. Concretamente se encarga de especificar los requisitos y suministrar una especie de manual para llevar a cabo la auditoría y la certificación
ISO/IEC 27009, Tecnología de la información - Técnicas de seguridad - Aplicación específica para cada sector de la norma ISO/IEC 27001 - Requisitos, se une a la familia de normas ISO/IEC 27000 para ayudar a maximizar la eficacia de la ISO/IEC 27001. Explica cómo incluir requisitos y controles adicionales a los de la ISO/IEC 27001 que son aplicables a sectores específicos, permitiendo lograr la coherencia en el desarrollo de normas

RIGE A LOS PROCESOS
Transmision de Datos
Transmision de Datos
Transmision de Datos
Transmision de Datos
Transmision de Datos
Transmision de Datos
Transmision de Datos
Transmision de Datos
Transmision de Datos
Transmision de Datos

Transmision de Datos
Transmision de Datos
Transmision de Datos
Transmision de Datos
Transmision de Datos
Transmision de Datos
Responsabilidad social
Sistemas de gestion de la informacion
Sistemas de gestion de la informacion
Sistemas de gestion de la informacion

Historia

PROCEDIMMIENTO DE AUDITORIA

HISTORIA

Versión	Fecha	Cambios Introducidos
1.0.0	**12/10/2022**	**Versión Inicial del Documento.**

TABLA DE CONTENIDOS

1. ALCANCE

El presente documento hace parte de la documentación mínima para realizar un buen diseño del SGSI basado en la norma ISO 27001:2013, este se aplicará a todas las áreas de la empresa OBSS INGENIERÍA que realicen procesos comprendidos dentro del alcance del SGSI.

2. OBJETIVO

Determinar globalmente que el estado actual de la gestión de la seguridad de la información para OBSS INGENIERÍA cumpla con los procesos definidos, teniendo en cuenta la norma ISO/IEC 27001:2013. El informe final determinará cuales serán los correctivos y las oportunidades de mejora que se deban aplicar y que OBSS INGENIERÍA deberá dar a estricto cumplimiento.

3. EQUIPO AUDITOR

Para OBSS INGENIERÍA debe ser claro que debe establecer y consolidar un equipo auditor, el cual deberá estar compuesto por personal calificado y que cuente con la experiencia requerida para dar cumplimiento a la toma de decisiones, el equipo debe contar con el siguiente perfil:

- Título universitario en Ingeniería Informática o Telecomunicaciones. Experiencia mínima de dos años en los sistemas y procedimientos a auditar.
- Curso en auditoría interna ISO/IEC 27001

3.1 HABILIDADES

- El Equipo auditor de OBSS INGENIERÍA deberá tener Independencia en las actuaciones de auditoría.
- El Equipo auditor de OBSS INGENIERÍA deberá tener Persistencia y tenacidad orientada a la consecución de los objetivos de la auditoria.
- El Equipo auditor de OBSS INGENIERÍA deberá tener Buenas habilidades sociales.
- El Equipo auditor de OBSS INGENIERÍA deberá tener una actitud positiva y abierta que le permita considerar ideas o puntos de vistas alternativas.
- El Equipo auditor de OBSS INGENIERÍA deberá tener Capacidad de trabajo en equipo.
- El Equipo auditor de OBSS INGENIERÍA deberá tener Dotes de gestión.

3.2 COMPOSICIÓN DEL EQUIPO AUDITOR.

El equipo auditor de OBSS INGENIERÍA debe ser consolidado y deberá estar compuesto por los siguientes roles:

- **Un Auditor jefe:** Persona del grupo que atesora la mayor experiencia y es capaz de coordinar a un equipo auditor. Debe tener conocimiento de todos los sistemas y procesos a auditar.
- **Dos Auditores:** Personas del grupo que cuentan con la formación y habilidades anteriormente descritas.
- **Expertos técnicos:** Gente experta en determinados procesos y sistemas que asesoran al auditor jefe y a los auditores donde no lleguen sus conocimientos técnicos.

4 PLAN DE AUDITORÍA

OBSS INGENIERÍA está en una primera fase de diseño del SGSI basado en la norma ISO 27001:2013, es importante sin embargo dejar claro que una vez la empresa se encuentre en la facultad de la implementación y posterior certificación, deberá llevar distintas auditorias internas que satisfagan con el objetivo como es la mejora continua y la renovación de la certificación. Por lo que OBSS INGENIERÍA determinará si cumple con la revisión por lo menos de una vez al año cada uno de los procesos y los sistemas del SGSI, en 4 auditorias trimestrales. (Conde, 2019)

A continuación, se detalla los planes que se deben llevar a cabo por trimestre para dar cumplimiento a una buena auditoria una vez OBSS INGENIERÍA tenga implementado el SGSI.

4.1 PRIMER TRIMESTRE

• Auditoría de los accesos físicos a los edificios.

• Auditoría de la seguridad física de los sistemas.

• Auditoría de la seguridad física de las dependencia críticas o restringidas

• Auditoría de la seguridad física de la información

• Supervisión las acciones llevadas a cabo para corregir las no conformidades detectadas en auditorías previas.

• Revisión de la política de seguridad de la organización.

4.2 SEGUNDO TRIMESTRE

• Auditoría de la seguridad de la red de la empresa

• Auditoría del acceso y uso de Internet

• Auditoría de conexiones con terceros

• Auditoría de Correo Electrónico corporativo.

• Supervisión las acciones llevadas a cabo para corregir las no conformidades detectadas en auditorías previas.

• Revisión de la política de seguridad de la organización.

4.3 TERCER TRIMESTRE

• Auditoría de configuración de los sistemas

• Auditoría de proceso de adquisición de Hardware y Software

• Auditoría de administración hardware y software

• Auditoría de desarrollo software.

• Supervisión las acciones llevadas a cabo para corregir las no conformidades detectadas en auditorías previas.

• Revisión de la política de seguridad de la organización.

4.4 TERCER TRIMESTRE

• Auditoría de almacenamiento de la información

• Auditoría de acceso lógico

• Supervisión las acciones llevadas a cabo para corregir las no conformidades detectadas en auditorías previas.

• Revisión de la política de seguridad de la organización.

5 MODELO DE INFORME DE AUDITORÍA.

Por ahora se indica a OBSS INGENIERÍA, que por ser parte de un diseño del sistema de gestión de la información basado en la norma ISO 270001:2013, no se establecerán formatos o modelos de auditoría, sin embargo, se da con ejemplo el siguiente formato para que tengan como base para cuando lleven a cabo la respectiva implementación.

PAG 1 DE 2 **indicar la versión del Documento** **Indicar el código de Auditoria**	**INFORME DE AUDITORIA INTERNA**	

1, DATOS	
Trimestre y año de Auditoría	
Norma de referencia	
Lugar de la auditoría	
Componentes del equipo auditoria	

2. ALCANCE	
EXCLUSIONES	

3. DEFINICIONES

4. OBJETIVOS

5. RESULTADOS

6. Observaciones y Oportunidades de Mejora

6. CONCLUSIONES

Bibliografía

Conde, L. R. (2019). *Anexo B – Procedimiento de Auditoría.* mistic.

https://www.iso27000.es/iso27002_15.html. (01 de 04 de 2022). *ISO 27001 ES.* Obtenido de ISO 27001 ES: https://www.iso27000.es/iso27002_15.html

Relación con proveedores. (21 de 05 de 2020). Obtenido de Relación con proveedores: https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/relacion-proveedores.pdf