DISEÑO DE SGSI BASADO EN LA NORMA INTE/ISO/IEC 27001:2013

PRESENTADO POR:
LEIDY CUBILLOS POVEDA
HAROLD FABIAN CHILATRA

ASESOR TÉCNICO DE PROYECTO:
JAVIER LEONARDO DIAZ

UNIVERSIDAD EL BOSQUE
FACULTAD DE INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD DE REDES TELEMÁTICAS
BOGOTÁ, COLOMBIA
18-12-2022

RESUMEN

OBSS INGENIERÍA es una empresa que tiene como objeto suministrar servicios de internet a través de radioenlaces, su actividad surge principalmente de necesidad de acceso a internet por parte de empresas u hogares en los que su ubicación geográfica no es favorable en términos de cobertura para contratar este servicio con proveedores convencionales que cuentan con redes en fibra óptica y es por esta razón que OBSS INGENIERÍA logra una amplia acogida con las diferentes alternativas tecnológicas para lograr transportar la información y cubrir con la necesidad del acceso a internet.

Frente a la prestación de este servicio OBSS INGENIERÍA tiene una responsabilidad adicional que consiste en garantizar la integridad, la confidencialidad y disponibilidad de la información, de aquí el interés y la iniciativa por parte de OBSS INGENIERÍA de contar con un diseño de Sistema de gestión de seguridad de la información el permita definir los lineamientos que debe seguir la organización en términos de seguridad bajo estándares internacionales. OBSS INGENIERÍA comprende que en el ejercicio de proveer los servicios de internet es necesario implementar herramientas y procesos que le permitan a la organización conocer cómo actuar frente de responsabilidad de salvaguardar la información no solo de la organización sino también del cliente finales.

PALABRAS CLAVE

SGSI, Activos, ISO 27001, Radioenlaces, Riesgo, Impacto, Vulnerabilidades, Amenazas, Controles, Confidencialidad, Integridad, Disponibilidad, Seguridad de la Información, Diseño.

ABSTRACT

OBSS INGENIERÍA is a company that has objetive to provide internet services through radio links, its activity mainly from the need for internet access by companies or homes in which their geographical location is not favorable in terms of coverage to contract this service. with conventional providers that have fiber optic networks and it is for this reason that OBSS INGENIERÍA achieves a wide acceptance with the different technological alternatives to transport information and cover the need for internet access.

Faced with the provision of this service, OBSS INGENIERÍA has an additional responsibility that consists of guaranteeing the integrity, confidentiality and availability of information, hence the interest and initiative on the part of OBSS INGENIERÍA to have a Security Management System design for the information allows defining the guidelines that the organization must follow in terms of security under international standards. OBSS INGENIERÍA understands that in the exercise of providing Internet services it is necessary to implement tools and processes that allow the organization to know how to act in the face of responsibility to safeguard the information not only of the organization but also of the end customers.

KEYWORDS

ISMS, Assets, ISO 27001, Radio links, Risk, Impact, Vulnerabilities, Threats, Controls, Confidentiality, Integrity, Availability, Information Security, Design.

Tabla de contenido

Lista de Tablas

Lista de Ilustraciones

1. Título

DISEÑO DE SGSI BASADO EN LA NORMA INTE/ISO/IEC 27001:2013

2. Introducción

Actualmente OBBS INGENIERÍA es una empresa dedicada a distribución de servicios de internet dedicado a través de radioenlaces principalmente para el segmento pymes. Su arquitectura técnica poco a poco ha ido creciendo y ha permitido un despliegue importante de cobertura mediante la implementación de nuevos nodos distribuidos en el departamento del Tolima. OBBS INGENIERÍA fue fundada en el año 2018 y ha venido sumando importancia dentro de la empresa que se dedican a comercialización de este tipo de servicios de telecomunicaciones, puesto que se ha preocupado por brindar acceso a internet en zonas de difícil acceso a muy bajo costo. Uno de los pilares de la empresa es fundamentado en que el internet se ha convertido en un servicio prácticamente indispensable en los hogares y por supuesto en las empresas, de esta misma forma a generado crecimiento en las organizaciones que lo proveen, generando un beneficio de manera bidireccional. Cuando hablamos de crecimiento no nos referimos solamente al aumento de ingresos de la compañía sino también al crecimiento de los activos de la organización los cuales son necesarios para aumentar la producción, en este caso el despliegue de la red para poder brindar servicio a muchos más usuarios.

Si bien OBSS INGENIERÍA viene experimentando este crecimiento, existe una gran preocupación que de cierta manera limita las proyecciones de la organización. Aunque es una empresa constituida legalmente ante cámara de comercio que realiza el pago de los impuestos, existe una falencia que se considera "normal" dentro de las organizaciones que apenas inician en la distribución de servicios de Telecomunicaciones y es el cumplimento de las normas y políticas definidas por la norma ISO:27001 y sus guías para los sistemas de seguridad de la información. De esta falencia surge la razón principal del desarrollo de este proyecto, la cual consiste en el diseño de un sistema de SGSI basado en la norma ISO 27001.

El propósito fundamental es realizar un análisis de estado actual de la organización y a partir del diagnóstico construir el SGSI con el objetivo de la empresa haga su implementación y continue con las recomendaciones de monitoreo y mejora continua que propone la norma.

3. Descripción general del proyecto

3.1 Definición del problema

Dado el crecimiento exponencial que ha tenido OBBS en el sector de las Telecomunicaciones, la vinculación de nuevos usuarios y despliegue de su red; surge la necesidad de garantizar la seguridad de información en toda la cadena de procesos para la planificación de los proyectos de conectividad que implementa OBSS INGENIERÍA, la poca experiencia y la desinformación respecto al funcionamiento de un SGSI hace tomar conciencia a la empresa que se debe considerar un diseño de los sistemas de información basado en la norma ISO 27001 y sus guías, dado que la información que manejan es de carácter confidencial y la empresa debe asumir la responsabilidad de la integración de este tipo de prácticas para contrarrestar los efectos de un sistema vulnerable y expuesto a los ciber atacantes.

La información confidencial que OBSS INGENIERÍA maneja se resumen en los contratos con clientes tanto de sector público como privado, la contratación directa con los proveedores ISPs, ser un proveedor de servicios de Internet con lleva una gran responsabilidad ya que a su vez los clientes acceden a la internet y pueden llegar a ser vulnerados en cualquier momento. Si OBSS INGENIERÍA no desarrolla la práctica de un sistema o procedimientos fijos y definidos que con lleven a organizar de manera adecuada todos esos procedimientos de seguridad y se pueda garantizar el pilar de la seguridad que son la confidencialidad, integridad y disponibilidad de la información, para ello es de vital importancia el diseño de un SGSI para proteger y minimizar todos los riesgos a los que OBSS INGENIERÍA pueda llevar a estar expuesta y que también cuando sucedan estos riesgos, se tengan los procedimientos claros para darle el respectivo tratamiento adecuado de la información a OBSS INGENIERÍA.

3.2 Aspectos a solucionar

- OBSS INGENIERÍA no cuenta hoy en día con un proceso a nivel de seguridad en la implementación de los servicios de internet que proveen a entidades privadas y gubernamentales.

- La organización a nivel de seguridad solo cuenta con un firewall perimetral, y no existen mecanismos adicionales que permitan asegurar la protección de la información.

- Los nodos que hacen parte del sistema de transmisión están físicamente expuestos y esto aumenta el porcentaje del riesgo sobre los activos de la organización.

- La organización se ve fuertemente impactada, porque el medio de transmisión dedatos está saturado de emisiones de ondas electromagnéticas que provienen de servicios que operan en la banda libre.

- Actualmente la organización no cuenta con una consultoría para el desarrollo de las buenas prácticas referente al uso de la seguridad de la información en cada una de las fases en la implementación de un proyecto.

3.3 Solución propuesta

La solución propuesta contempla los requerimientos mínimos para el para el diseño de SGSI, tomando como punto de referencia el diagnóstico del estado de la seguridad de la información de OBSS INGENIERÍA. La propuesta cuenta con un documento estructurado con las mejores prácticas de la seguridad de la información, estandarización de procesos y formatos a nivel de diseño para que la entidad posteriormente pueda certificarse en la norma ISO 27001.

La solución está constituida por 4 pasos principales: el primero consiste en el diagnóstico y levantamiento de la información de la organización en materia de seguridad, el segundo corresponde al análisis de la información recopilada, el tercer paso el diseño y estructuración de los controles y planes de mejora, finalmente la documentación de toda la información necesaria para que OBSS pueda implementar el SGSI.

Ilustración 1 El proceso de la seguridad de la información *[1]*

OBBS reconoce su desconocimiento de mejores prácticas para la seguridad de la información y en base a ello inicia la búsqueda de profesionales que puedan orientar la organización en el uso herramientas, políticas y normativas necesarias para garantizar la seguridad de la información.

4. Estado del arte

Para definir cada uno de los objetivos que se proponen para el diseño de un SGSI para la empresaOBSS INGENIERÍA, se seguirá una metodología de investigación y levantamiento de información relacionada con proyectos orientadas y basados en la norma ISO/IEC 27001, con el fin de atender la necesidad de un diseño de SGSI dentro de una organización y bajo recomendaciones contenidas en la normaISO 27001 y sus guías. Se realizó la investigación de proyectos que se implementaron, diseñarony ejecutaron en diferentes organizaciones a nivel nacional e internaciones donde el objetivo principal está basado en el uso de las buenas prácticas de la seguridad de la información.

El proyecto de grado "propuesta de implementación de un sistema de gestión de seguridad de la información basado en la norma iso 27001:2013 para la empresa lovato city gas s.a.", que fue realizado por Liz Mayoly Esguerra cruz y Geraldine Alejandra ortiz cárdenas de la Universidad Francisco José de Caldas", para el cual plantearon la creación de una propuesta de proyecto el cual está enmarcado en el establecimiento del SGSI para procesos que corresponden al área de tecnología.

El proyecto de grado "diseño de un sistema de gestión de seguridad de la información (sgsi) basado en la norma ntc iso/iec 27001:2013 en el área de desarrollo de la empresa ikatech solutions". Realizado por Cristian Eduardo Garcia Sánchez, Nicolás esteban forero Gonzales, maría Fernanda Bojacá bonilla, de la Universidad Cooperativa de Colombia, para la cual plantearon analizar los procesos relacionados a la seguridad de la información que se puedan implementar en Asesorías y consultorías Jurídicas S.A.S, para poder establecer un sistema de gestión de seguridad de la información, de forma que la compañía pueda cumplir con los estándares que integran los principios de SGSI.

4.1 Marco de referencia teórico

El Sistema de Gestión de Seguridad de la Información (SGSI) permite gestionar de manera adecuada la seguridad de la información institucional, a fin de hacer frente a amenazas de ataqueo intromisión, error, actos fortuitos (inundación, incendio, etc.), entre otros.

El SGSI tiene entre sus tareas, Reunir los procesos para gestionar de forma eficiente la accesibilidad de la información institucional, Asegurar la confidencialidad, la integridad y la disponibilidad de los activos de información, es decir, los recursos de información con los que laboramos y Minimizar riesgos de seguridad de la información para lograr el cumplimiento de nuestras funciones y metas.

4.1.1 Reduce los riesgos de seguridad de la información

- Mejorar la seguridad de la información en el ambiente actual y hacer énfasis en el control de la seguridad de la información de acuerdo con el negocio, actualizando las políticas de la seguridad de la información, controles logrando proporcionar e incentivar la revisión y actualización periódica de los controles de seguridad de la información.

- Reducir de manera integral la probabilidad de amenazas a la seguridad de la información o vulnerabilidades no identificadas.

- Un enfoque sólido, estandarizado y profesional para la gestión de riesgos que brinda consistencia en múltiples sistemas a lo largo del tiempo y aborda de manera consistente los riesgos de seguridad de la información (un enfoque basado en el riesgo se enfoca en las áreas de mayor riesgo)

- Mayor capacidad para transferir selectivamente el riesgo a las aseguradoras y permitir la negociación de primas más bajas a través de los controles establecidos

- Los administradores y empleados se familiarizarán cada vez más con la terminología y los controles de seguridad de la información.

4.1.2 Beneficios de la estandarización

- Proporcionar un "terreno común": Una base sólida sobre la que se construya controles adicionales y específicos del sistema sin presentar ninguna modificación al control básico.

- Evitar la especificación, revisión y aplicación por separado los requisitos básicos de referencia para el control de cada sistema.

- Permite la reutilización de recursos para las diferentes áreas de la organización sin generar cambios o traumatismos en la operación.

- La organización tiene como pilar fundamental sedimentar los esfuerzos y recursos que satisfacen los controles básicos.

- Tener identificado las buenas prácticas que sean reconocidas y aceptadas en la política de la seguridad de la información.

- Lograr una buena optimización en tiempo y dinero mediante la aceptación de buenas prácticas.

- Proporcionar términos comunes que permitan debatir, establecer, desplegar y valorar las necesidades en seguridad de la información y los controles necesarios.

- ISO/IEC 27002 es un estándar para los diferentes controles de seguridad de la información y proporcionar una base sólida para evaluar el riesgo y aplicar los controles adecuados.
- Suministrar el impulso necesario para evaluar los sistemas, datos y flujos de la información para minimizar la duplicidad y otros procesos innecesarios para lograr una mejor calidad de la información (reingeniería de los procesos de negocio) - ahorro de costes.

- Proporcionar una métrica para medir el rendimiento y aumentar proporcionalmente la línea base para la seguridad de la información.

- Después de haber aplicado las normas ISO/IEC 27001, la organización tendrá una política más formal sobre los procedimientos que deben tener en cuenta para la seguridad de la información, la cual les permitirá ser adaptativo para el personal en general.

4.1.3 Beneficios de la certificación

- Resolver las solicitudes y peticiones de los clientes, proveedores con el fin de acoplarse a los controles de seguridad de lainformación de la organización sin necesidad de atender consultas individuales que afecte la confidencialidad de la información.

- Proporcionar un modelo de seguridad de la información que sea estándar y permita evaluar la calidad de los controles en los clientes finales, proveedores y contratistas.

- El no cumplimiento de las normas ISO/IEC 27001 se puede interpretar como un puede ser tomado como una señal de vulnerabilidad. Para ello es importante poder Certificar a futuro el cumplimiento de esta norma para que se pueda promover la imagen de la empresa en el departamento del Tolima y se convierta en un socio estratégico para las empresas tanto del sector público como privado.

- Garantizar a todos los interesados en el caso de negocio que la organización está trabajando para la minimización de los riesgos que estén asociados a la seguridad de la información, esto con el total compromiso en la adaptabilidad de la norma ISO 27001.

- Potencialmente reduce o restringe las quejas de terceras partes en caso de fallos de seguridadde información - ahorro de costes y reducción de riesgos

4.2 Marco de referencia tecnológico

La norma ISO 27011 plantea diferentes directrices en la gestión de seguridad para las compañías u organizaciones que estén en el sector de las telecomunicaciones y estás a su vez se basan en la norma ISO 27002. La norma permite establecer y aplicar los controles más modernos en cualquier tipo de organización que tenga interés en salvaguardar la información.

La información de las organizaciones de telecomunicaciones es un activo crítico y, por lo tanto, es necesario preservarla, ya que también es objeto de muchas amenazas. Por todo ello, los objetivos de esta Norma Internacional son: Lograr la seguridad de la información a través de prácticas que den confianza en las actividades que realiza una organización. El desafío global de la seguridad de la información es específico de estas empresas.

La norma ISO27011 garantiza la seguridad de la información de la empresa a través de los controles adecuados. Estos controles deben implementarse, controlarse, especificarse y deben evolucionar con el tiempo para cumplir con los objetivos de seguridad establecidos previamente por estas entidades. Las organizaciones de telecomunicaciones deben determinar los requisitos y evaluar continuamente los posibles riesgos de seguridad antes de seleccionar los controles. La elección de estos controles dependerá de la aceptación de los riesgos planteados a la organización y, además, de la necesidad de cumplir con leyes y reglamentos internacionales o no relacionados. Con la implementación del estándar ISO-27011, las organizaciones que trabajan en telecomunicaciones deben hacer cumplir las siguientes pautas: Proteger la integridad, confidencialidad y disponibilidad de la infraestructura y los servicios. Garantizar la eliminación de riesgos de los servicios prestados por las empresas de telecomunicaciones a través de un sólido proceso de asociación. Deben saber reorganizar los recursos para que las actividades se realicen de manera más eficiente. Aceptar los principios globales relacionados con la seguridad de la información. Tiene la capacidad de elevar la moral y la confianza. ISOTools es una plataforma tecnológica que ayuda a las organizaciones a implementar la norma ISO 27011, y, además, proporciona una serie de aplicaciones para el diagnóstico de seguridad de la información, como el control de riesgos.

5. Glosario de términos

Amenazas: [1]Las amenazas de seguridad de la información o ciber amenazas corresponde a un evento potencial que pueden afectar negativamente a las operaciones de una organización o a sus activos, "a través del acceso no autorizado a un sistema de información, la destrucción, divulgación o modificación de información y/o la denegación de servicio".

Confidencialidad: [2]La confidencialidad de la información asegura que el acceso a ésta sea únicamente por aquellas personas que tengan autorización para hacerlo, evitando que ésta sea divulgada, comunicada, robada, saboteada por personas o sistemas no autorizados.

Disponibilidad: Se refiere a que la información debe encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos, aplicaciones, y el acceso a ésta debe hacerse por personas autorizadas.

Extracción de la información: La extracción o fuga de información se clasifica como un incidente de seguridad cuando personas ajenas a la organización sustraen información confidencial.

Integridad: Mantener la integridad de la información se refiere, no solo a la información almacenada en el equipo de cómputo, sino también a la que se encuentra en los respaldos, documentos, reportes, etc. La integridad consiste en proteger la información contra la lectura noautorizada.

Radio Enlaces[3]: Un radioenlace es un sistema electrónico de comunicación inalámbrica medianteondas de radio que permite la transferencia de información entre dos o más puntos.

Riesgos: [4]Es la combinación de las consecuencias de un suceso de seguridad de la información y la probabilidad de ocurrencia asociada. Así mismo, está asociado con la probabilidad de que las amenazas exploten vulnerabilidades de un activo de información o grupo de activos de información y por lo tanto causar un daño a la organización.

Sistema de Información[5]: Un sistema de información es un conjunto de elementos orientadosal tratamiento y administración de datos e información, organizados y listos para su uso posterior,

generados para cubrir una necesidad u objetivo.

Vulnerabilidad: Es una debilidad presente en un sistema operativo, software o sistema que le permite a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones.

[1] https://www.ealde.es/ataque-amenaza-vulnerabilidad-ciberseguridad/

[2]Principios de Seguridad Informática en Sistemas de Información
https://www.uaeh.edu.mx/scige/boletin/tlahuelilpan/n6/e5.html

[3] https://www.prored.es/que-es-un-radioenlace/

[4] https://www.ldgrupo.com.pe/que-es-el-riesgo-de-seguridad-de-informacion/

[5] https://www.uaeh.edu.mx/scige/boletin/tlahuelilpan/n6/e5.html

6. Justificación

El activo más importante de una organización es la información y hoy en día se vuelve prioridad de las empresas la seguridad de la información. La globalización y la transformación digital en la que actualmente vivimos hace que los ataques informáticos estén en aumento por lo que las empresas emprenden una carrera en llevar a cabo diseños e implementación de normas que le permitan garantizar el cuidado ya sea de sus activos o los servicios que proveen para asegurar la cadena de producción. Si bien OBSS INGENIERÍA no ha sido víctima de ataques informáticos sabe que tienen un alto riesgo de vulnerabilidad en sus sistemas de información.

OBSS INGENIERÍA es una organización proveedora de servicios de Telecomunicaciones y dentro de sus principios esta garantizar la confidencialidad, la disponibilidad y la integridad de la información tanto de la organización como de los servicios que provee. Es por esta razón que surge de la necesidad de diseñar un SGSI que permita definir, documentar los controles y procesos a seguir en materia de seguridad para garantizar cumplimientos o requisitos en la participación de licitaciones tanto de sector gobierno o privado para la prestación adecuada de servicios de radioenlaces.

OBSS INGENIERÍA en una empresa joven en el negocio de Telecomunicaciones, ha tenido gran acogida en el departamento del Tolima y ha logrado solidificarse financieramente. En este momento su preocupación radica en establecer medidas y controles atendiendo a las normas actuales que buscan dar cumplimiento a la protección de la información, Adicionalmente OBSS INGENIERÍA busca la estandarización de procesos para optimizar tiempos, costos y metodologías del diseño de proyectos.

7. Objetivos

7.1. General

Diseñar el sistema de Gestión de Seguridad de la Información en la empresa OBSS INGENIERÍA,basados en la norma técnica colombiana GT ISO/IEC 27001 para la transmisión de datos en radio enlace.

7.2. Específicos

- Identificar cuáles son las necesidades de la empresa OBSS INGENIERÍA para estructurar el diseño del SGSI en los sistemas de transmisión de datos mediante radio enlaces.

- Definir el estado actual de la seguridad de la información en el sistema de transmisión de datos mediante radio enlaces de la empresa OBSS INGENIERÍA.

- Describir cuales son los riesgos y amenazas dentro de los sistemas de informaciónpara determinar su impacto en los sistemas de transmisión de datos de radio enlaces.

- Documentar los controles de seguridad de la información con la norma NTC-ISO/IEC 27001 para los sistemas de transmisión de datos de radio enlaces.

8. Requerimientos

8.1 Requerimientos Funcionales

- Diseñar formatos y documentos teniendo como base la normatividad ISO 27001:2013, con el fin de garantizar que esta sea implementada por el profesional de seguridad de la información designado por OBSS INGENIERÍA.
- Realizar la identificación de los activos fijos de la compañía para estructurar los entregables mínimos aprobados por la alta gerencia acorde a la norma ISO 27001:2013.
- Identificar y analizar los riesgos para construir el plan del tratamiento del riesgo para OBSS INGENIERÍA, teniendo en cuenta la norma ISO 27001:2013.

8.2 Requerimientos No Funcionales

- Todas las políticas y procesos definidos dentro del diseño del SGSI debe desarrollarse bajo un ciclo iterativo que permita afinar su aplicabilidad dentro de las distintas áreas de la organización.
- La documentación suministrada a la compañía corresponde a los requisitos mínimos exigidos por la norma ISO 27001:2013, sin embargo, OBSS INGENIERÍA podrá modificar tanto los formatos y documentos de acuerdo con los lineamientos y actualizaciones que emita la norma.

8.3 Requerimientos de restricción

- Se estimo el cronograma y presupuesto, el cual estará sujeto a la aprobación financiera y de la alta gerencia de OBSS INGENIERÍA, para la ejecución de este.
- Solo será suministrado a OBSS INGENIERÍA, el diseño que contiene los planes de mejora y los documentos correspondientes; la implementación y actualización estará a cargo de OBSS INGENIERÍA acorde al cronograma sugerido.

9. Metodología

Para el diseño del SGSI aplicado a la transmisión de datos de radios enlaces en empresa OBSS INGENIERÍA lo segmentaremos en varias fases:

La primera fase será realizar un análisis que permita identificar la necesidad de la empresa OBSS INGENIERÍA en materia de seguridad de la información enfocado en el proceso que conlleva a la transmisión de datos a través del espectro radioeléctrico desde el centro de datos de la organización hasta el usuario final.

En la segunda fase evaluaremos el estado del cumplimiento actual de los controles de seguridad a los que aplica la organización en el proceso de trasmisión de datos a través de radioenlaces, esto en función de los lineamientos que dicta la norma ISO 27001 en el anexo A, dominio y controles.

En la tercera fase recopilaremos los riegos a los que está expuesto la organización al no contar con un SGSI, se analizará el impacto y la criticidad del riesgo, esto con el fin de consolidar un diagnóstico más de detallado respecto al estado actual de la organización en el ejercicio de preservar la seguridad de la información. Para ello se trabajó con metodología de la guía 27005, esta pertenece a la familia de las ISO 27000 la cual se basa en la gestión de los riesgos de la información teniendo en cuenta los activos de la empresa.

Finalizaremos con la cuarta fase con la documentación de todos los procesos, formatos y metodologías que debe seguir OBSS INGENIERÍA en uso de las buenas prácticas para garantizar la seguridad de la información, entregaremos a la organización un documento estructurado con los requisitos que sugiere la norma ISO 27001 y sus guías para el diseño de un SGSI.

9. Documentación requerida para el buen diseño de la Norma ISO 27001 (Revisión 2013).

OBSS INGENIERÍA quiere en caminarse a la acreditación en ISO 27001, como se ha mencionado anteriormente es importante la protección de la información sensible de la que la empresa OBSS INGENIERÍA dispone. Al llegar a implementar y acreditar en ISO 27001, los clientes de OBSS INGENIERÍA tanto actuales como futuros podrán estar más confiados en que la seguridad de su información no será revelada y que cuenta con los más altos estándares de protección de la información, por tratarse de una norma internacional y que pocas empresas como OBSS INGENIERÍA no tienen dicha certificación.

En el desarrollo de todo el diseño de la norma ISO 27001:2013 para la empresa OBSS INGENIERÍA, se toma como base la lista de muestra del conjunto mínimo de documentos y registros requeridos por la ISO/IEC 27001:2013. [2]

Documents*	ISO 27001:2013 clause number
Scope of the ISMS	4.3
Information security policy and objectives	5.2, 6.2
Risk assessment and risk treatment methodology	6.1.2
Statement of Applicability	6.1.3 d)
Risk treatment plan	6.1.3 e), 6.2
Risk assessment and risk treatment report	8.2, 8.3
Definition of security roles and responsibilities	A.7.1.2, A.13.2.4
Inventory of assets	A.8.1.1
Acceptable use of assets	A.8.1.3
Access control policy	A.9.1.1
Operating procedures for IT management	A.12.1.1
Secure system engineering principles	A.14.2.5
Supplier security policy	A.15.1.1
Incident management procedure	A.16.1.5
Business continuity procedures	A.17.1.2
Legal, regulatory, and contractual requirements	A.18.1.1

Ilustración 2 Documentos Mínimos requeridos para Diseño de la norma ISO 27001:2013

- **¿Cómo se beneficia OBSS INGENIERÍA?**

El tener la implementación y acreditación de la ISO 27001, tiene varios beneficios en los que brindará confianza tanto a los empleados y clientes. Estos beneficios son:

- Trabajar con un proveedor de Servicios fiable que asegura y mantiene que la integridad de todos los datos tanto de los empleados como el de sus clientes estén seguros.

- Que el personal de OBSS INGENIERÍA, se encuentre en la respectiva capacidad de seguir las reglas necesarias para garantizar la protección de los datos del negocio.

- Minimizar los riesgos como las amenazas de seguridad y evitar cualquier debilidad que pueda alterar la información de OBSS INGENIERÍA.

Para garantizar el correcto diseño de la Norma ISO 27001, es de vital importancia que se diseñe la documentación requerida y que permita a OBSS INGENIERÍA listar cada uno de los propósitos que conlleva buscar la certificación de la norma ISO 27001. De no hacerse de esta manera, podría dar lugar a la no conformidad de una buena implementación y posterior certificación.

Además, es importante que los documentos que son obligatorios para el cumplimiento del diseño y posterior implementación corresponden a la mejor práctica para que los auditores puedan observar lo que se ha realizado al interior de OBSS INGENIERÍA y que posteriormente se pondrá en la práctica.

Como OBB INGENIERÍA busca la respectiva implementación de la norma ISO 27001 por primera vez, debe por lo tanto seguir paso a paso la documentación, al inicio será un proceso desalentador, pero si OBBS INGENIERÍA, sigue a cabalidad será un éxito la implementación de la norma ISO 27001.

Ahora luego de que se han generado y gestionado toda la documentación para el respectivo cumplimiento del SGSI, a continuación, se lista los anexos que se entregarán a OBBS INGENIERÍA para que lo usen como plantilla de esta primer fase de diseño y que permita seguir las instrucciones y el uso de las herramientas de proyectos que van orientadas a la correcta

estructura de diseño de la norma 27001; siendo la opción más completa para que la documentación permita a OBSS INGENIERÍA disminuir los tiempos en la respectiva implementación y así aliviar los riesgos que conlleva un proyecto de estos, y lograr la optimización del cumplimiento de toda la norma ISO 27001.

9.1 Scope SGSI.

Para la estructuración del alcance SGSI a presentar a la empresa OBBS INGENIERÍA se inicia con un acercamiento con el equipo gerencial de la organización para entender y estructurar el plan de trabajo a llevar a cabo en el objeto de construir el diseño del SGSI basado en la norma ISO 27001. Posteriormente se realizó una reunión presencial con el equipo técnico a fin de conocer el modelo de negocio y la infraestructura técnica de radioenlaces que hoy en día opera en OBSS INGENIERÍA para la prestación de los servicios de conexión a internet a cliente final.

Finalmente se definen las bases, requisitos mínimos a cumplir y lineamientos a seguir teniendo en cuenta el diseño del SGSI, analizando los procesos más críticos en la seguridad de la información con el servicio que presta actualmente por medio de radioenlaces.

9.2 Política y Objetivos de la seguridad de la información.

El documento de política de seguridad de la información tiene como objetivo delinear los requerimientos que son fundamentales para OBSS INGENIERÍA y que debe cumplir con respecto a la Seguridad de todo el sistema de información.

Esta política engloba los aspectos que son importantes en OBSS INGENIERÍA, allí se incluye el hardware y software, los recursos humanos y el control de acceso. Es importante dejar de manera clara a OBSS INGENIERÍA, que esta política debe estar en constante actualización y revisión para que las demandas cambiantes de la industria y más para el servicio que provee OBSS INGENIERÍA. [3]

El documento detalla los objetivos de OBSS INGENIERÍA, y posteriormente cuales son los pasos que los empleados deben seguir para lograr los objetivos, al igual que todo lo referente a los roles y responsabilidad estarán estrictamente definidos. [3]

Para que la política sea exitosa se debe describir cada uno de los activos de OBSS INGENIERÍA, ya que se determinará como se llevará acabo la administración de cada uno y quien será el responsable del control. Cabe recordar que el objetivo más importante de un programa de seguridad como el que se está diseñando para OBSS INGENIERÍA se basa en la protección de la información y los activos dentro de la empresa, ya que se debe garantizar esta protección.

Algunos de los objetivos para garantizar la protección de la información y los Activos pueden ser;

- Garantizar que la información confidencial está protegida de personas no autorizados, tanto internas como externas a la empresa OBBS INGENIERÍA.
- Asegurar la integridad de la información, ya que esta debe ser confiable y precisa, esto se hace protegiéndola de manera segura para que ninguna persona altere o modifique la información sin ningún consentimiento.
- Considerar la disponibilidad de la información. Se debe asegurar que no cualquier persona de la empresa tenga acceso a los documentos que son confidenciales.

9.2.1 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.

9.2.2 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 triángulo 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.

9.2.3 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.

9.2.4 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.

9.3 Metodología de evaluación y tratamiento del riesgo.

Para llevar a cabo un proceso de gestión de riesgos es importante la definición de la metodología que se va a seguir, y también definir el objetivo que corresponde al primer paso para que la empresa OBSS INGENIERÍA conozca la metodología y como la gestión de riesgo se hace de manera homogénea en todas las áreas de la empresa.

La definición de la evaluación de riesgos se puede hacer tanto cualitativa como cuantitativa. Si es de manera cualitativa se deben definir cuál será la escala para definir y los niveles de los que se considere un riesgo como aceptable o no aceptable. [4]

OBSS INGENIERÍA debe contar para la fase de diseño con el plan de gestión riesgos para que se pueda garantizar la continuidad del negocio. Por ello es importante que se desarrolle un análisis de riesgo de la seguridad de la información para OBSS INGENIERÍA, y se parte con el diseño, identificación y evaluación de la situación actual de los activos donde se describe las amenazas, para poder continuar con la medición de los riesgos existentes y luego sugerir como disminuir el riesgo se plantea la gestión de riesgos en la seguridad de la información. [5]

Dentro de la clasificación de los riesgos se puede medir riesgos por desastres ambientales, riesgos que pueden estar relacionados a los procesos no adecuados en el tratamiento de la información, desconocimiento de las respectivas normas y políticas de seguridad y el no cumplimiento a las políticas de seguridad, estas suelen las más frecuentes y las que generan un mayor impacto para las empresas, por ello para OBSS INGENIERÍA, los tratamientos de riesgos son fundamentales y que estén estructurados y documentados. Si una empresa como OBSS INGENIERÍA, no cuenta con un plan de riesgos podría estar expuesta a la pérdida de su información, la información de los clientes y sobre todo de cada uno de los empleados. [5]

Una vez se tenga identificados los riesgos, se procede a realizar cada uno de los análisis posibles de los problemas que se pueden ir presentando en la empresa. Para dejar documentado al detalle esta metodología, se realiza una evaluación y contabilización de todos los activos de OBSS INGENIERÍA, y se indican con las amenazas y debilidad a las que se podría ver enfrentado, y luego a ellos se procederá a dar la probabilidad con que este riesgo pueda suceder.

9.3 Estado de aplicabilidad.

El estado de aplicabilidad tiene una conexión entre la evaluación y el tratamiento de los riesgos de una empresa, por lo que es importante dejar muy claro que es un requisito para la futura implementación de ISO 27001 para OBSS INGENIERÍA.

El estado de aplicabilidad es un documento que debe estar actualizado continuamente en para proporcionar una definición detallada de cómo será tanto el diseño y posterior implementación de la seguridad de la información.

La preparación del estado de aplicabilidad debe tener un foco importante, dado que se requiere de una buena dedicación en tiempo, esfuerzo y compromiso desde OBSS INGENIERÍA, luego debe ser aprobado por la dirección de la empresa.

Los procesos para el diseño y posterior implementación del SGSI debe garantizar:

- Se debe documentar el método o proceso.
- Se debe contar con controles que se documenten.
- Se debe garantizar auditorias y revisiones constantes.

Para el análisis del estado de aplicabilidad se toma como base el documento Anexo A que contiene los 114 controles que sugiere la norma ISO 27001. Con esta información se determina de acuerdo con el trabajo mutuo entre OBSS INGENIERÍA y la consultoría realizada en el desarrollo del diseño del SGSI para definir el estado real de la organización frente al cumplimiento de todos los controles.

9.4 Plan de tratamiento del riesgo.

El plan de tratamiento del riesgo es parte fundamental del diseño de la norma ISO 27001, esto porque corresponde a un plan integral que permitirá implementar en esta etapa los controles que permitirán reducir la probabilidad del impacto de los riesgos. [6]

En el diseño de plan de tratamiento de riesgos debe garantizar que los procesos de tratamiento de riesgos se llevan a cabo, para que luego OBSS INGENIERÍA, pueda realizar una buena implementación, considerando un buen plan de tratamiento de riesgos.

Un plan de tratamiento de riesgos de la ISO 27001, debe listar la siguiente información que corresponde a:

- El resumen de la identificación del riesgo.
- Qué controles u otras actividades planea implementar
- Quién es responsable del diseño y posterior implementación.
- ¿Cuándo son los plazos para las actividades de tratamiento de riesgos?
- Qué recursos humanos y financieros son necesarios para la implementación
- Cómo juzgará si la implementación fue exitosa

Mitigar algunos riesgos puede ser un proyecto a más largo plazo que otros riesgos. Su plan de tratamiento de riesgos puede mostrar que el trabajo está en progreso. Puede documentar sus pasos y medidas provisionales.

9.5 Informe de Evaluación y tratamiento del riesgo.

El informe de la evaluación del riesgo es uno de los documentos más complejos tanto para el diseño e implementación de la ISO 27001, pues se debe evaluar y tratar el riesgo desde el inicio de proyecto de seguridad de la información, además que se deben establecer las bases correspondientes para lograr una gestión de la seguridad de la información para OBSS INGENIERÍA.

En la fase de diseño se establece como proceso principal la identificación de los bines que requieren protección; y se deben considerar cuales son las amenazas que pudiera ocurrir si se altera la confidencialidad, integridad o disponibilidad de la información, allí se evalua con que probabilidad puede ocurrir esta consecuencia de riesgo para cada activo y posterior se debe encontrar o identificar la manera más apropiada para prevenir ese riesgo, esto se hace detectándolo o tratando el riesgo. [7]

9.6 Definición de Roles y Responsabilidades

La política de definición de roles y responsabilidades es prioritaria en el diseño de la ISO 27001, ya que permite tener la respectiva comunicación efectiva y los estándares de seguridad de la información, además que se especifica cuáles serán los roles que estarán dentro de la organización donde se detallará las responsabilidades y cómo será la compresión para que se logre la respectiva protección de la información.

El propósito de la definición de roles y responsabilidades consiste en aclarar, coordinar las actividades, cuáles serán las acciones para que se difunda la política, los estándares y los lineamientos para el cumplimiento de esta cuando se encuentre en la etapa de implementación.

Esta política se aplica para cada uno de los roles de OBSS INGENIERÍA y contratistas que participen en el programa de seguridad de la información.

Es importante indicar que la identificación en la etapa de diseño de los roles que se requieren dentro de la empresa OBSS INGENIERÍA para garantizar las responsabilidades y que estén claramente definidas y así aclarar como cada rol va a cumplir con las responsabilidades en pro de la protección de la información.

9.7 Inventario de Activos.

La ISO 27001 define un activo como cualquier hardware o cualquier ubicación dentro de los sistemas de una empresa donde se almacena, procesa, o se accede a información confidencial de la empresa.

Por lo tanto, todo activo que haga parte en la transmisión o recepción de la información debe ser categorizado como un activo. Este activo también puede ser parte fundamental o de almacenamiento de información crítica para OBSS INGENIERÍA, como un servidor o sistemas de soporte define un activo como cualquier ubicación valiosa dentro de los sistemas de una organización donde se almacena, procesa o se puede acceder a información confidencial.

Los activos se pueden dividir en las siguientes categorías:

- Hardware (servidores informáticos, equipos de red, ordenadores, portátiles, etc.);
- Software;
- Información (registros en papel y digitales);
- Personas (empleados, contratistas, voluntarios y cualquier persona que conozca información confidencial);
- Servicios (prestados por la organización o por terceros); y
- Las ubicaciones (las instalaciones de la organización, las oficinas de los empleados remotos, etc.)

Para dar cumplimiento a la norma ISO 27001, se debe considerar un inventario de Activos actualizado de la empresa, donde se debe incluir tanto activos fijos o activos intangibles como datos personales. Este inventario de activos es de carácter primordial porque permite a la empresa administrarlos y así mismo mitigar los riesgos de seguridad de la información.

9.8 Política de Control de Acceso.

Esta política tiene un propósito y es el aseguramiento del acceso lógico como físico a la información y que los sistemas estén de manera controlada para garantizar la protección de los sistemas de información.

Esta política tiene un alcance muy importante ya que se da acceso a toda la información reservada, a todos los sistemas TIC de la empresa y a los accesos físicos, áreas y ubicaciones donde se encuentre información y datos que sean confidenciales.

La política se aplica a lo largo de ciclo de vida de la información, es decir desde la creación, utilización, almacenamiento y finalmente la eliminación.

9.9 Política de seguridad de Proveedores.

La política de seguridad de proveedores establece las condiciones para todos los servicios que son adquiridos por proveedores o terceros , la cual les indica cuales son las responsabilidades y los controles que permitan mitigar cualquier riesgo que involucre la información de la empresa, por lo que es importante siempre tener una copia, modificación, divulgación y destrucción no autorizada, que pueda llegar afectar la integridad, confidencialidad y disponibilidad de la información para OBSS INGENIERÍA.

Los requisitos que se deben cumplir para lograr mitigar los riesgos que estes asociados al acceso de la información de proveedores o terceros a los activos de OBSS INGENIERÍA, debe ser acordados en ambas partes para que se asegure la respectiva protección de los activos de la empresa.

Para ello los proveedores contaran con un acceso limitado a la información reservada y confidencia de la empresa. Si en algún momento se proporciona esta información al tercero el tercero debe firmar un compromiso con todas las medidas de seguridad donde se garantice la no divulgación o modificación de la información compartida. Otra medida importante es que los terceros no podrán tener permisos a las áreas donde se almacene información importante de la empresa o información que se sensible, por lo tanto, se debe limitar el acceso de ingreso a dichas áreas, si el proveedor transita por allí debe estar acompañado y con permiso escrito para la validación de esta información.

9.10 Política de gestión de incidentes.

La política de gestión de incidentes tiene como objeto que las acciones y procedimientos que tienen una empresa para recuperarse ante una interrupción de un servicio y que no esté planificada. Por lo que es importante que OBSS INGENIERÍA, tenga conocimiento del propósito de esta política, y es que todo procedimiento se debe planificar, responder, realizar gestión y escalamiento de cualquier incidente que sea crítico y afecte la disponibilidad del servicio y la operación de la empresa, logrando realizar mitigación.

9.11 Política de continuidad del negocio.

La política de continuidad del negocio o sistema de gestión de continuidad del negocio identifica como objetivo principal la capacidad que una empresa tiene para la prestación de servicios y así poder establecer los respectivos lineamientos en caso de una posible situación o situaciones que encadenen a la interrupción de los servicios que la empresa presta como línea base de su negocio. Para la gestión de continuidad del negocio, se identifican dos conceptos que son claves para lograr entender el concepto de gestión de continuidad.

Planificación de continuidad de negocio: Esta corresponde a una planificación estratégica que la empresa OBBS INGENIERÍA debe tener constituida para que cubra el negocio y garantice que cualquier función que sea critica esté disponible después de que se presente una falla, y permita que la operación no sufra mayores golpes en el desarrollo del negocio.

Plan de recuperación de desastres: Este plan debe ser estructurado y llevar la respectiva secuencia de actividades que se deben de llevar a cabo para lograr el respectivo restablecimiento de la operación del servicio que preste la empresa, garantizando que la operación continue en su curso normal.

Para garantizar una buena función de contingencia para la reducción de riesgos desde el diseño de la norma se debe definir un correcto proceso de gestión de continuidad. Para ello es importante conocer toda la infraestructura sobre la que se realizan o ejecutan los servicios que dan gran soporte de los procesos del negocio, es decir garantizando un inventario y una estructura de base de datos actualizada.

9.12 Normograma.

El normograma o la regulación y obligación contractual requerida, desde el punto de vista de la gestión de la seguridad de la información puede ser un gran reto dado que se debe especificar el panorama de las amenazas que están en constante actualización. Dentro de todos los requisitos obligatorios

Desde la perspectiva de la seguridad de la información, cumplir con las leyes, regulaciones y obligaciones contractuales requeridas puede ser un desafío tan grande como lidiar con el panorama de amenazas en constante evolución y las nuevas formas de ataques. Lo que muchas organizaciones no entienden es que ambos son igualmente importantes.

Son requisitos de adaptabilidad de la forma de leyes laborales, requisitos de seguridad relacionados con TI, derechos de propiedad intelectual/leyes de derechos de autor, privacidad, cifrado de datos y leyes de protección; esta lista interminable puede ser bastante intimidante. ¿Está tomando todas las medidas necesarias para garantizar que se cumplan las leyes y los reglamentos?

Las leyes y reglamentos son entidades vivas que pueden variar según la rama de la industria, el país y el tipo de información, entre otros aspectos. Dependiendo de su tipo de industria, su negocio puede estar bastante familiarizado con las regulaciones o ser completamente nuevo en ellas. La frecuencia de los incidentes relacionados con la seguridad y la magnitud de su impacto han hecho que los gobiernos de todo el mundo sean conscientes de la necesidad de proteger a las personas y las empresas contra el manejo inadecuado de la información confidencial.

Obviamente, este es un tema en evolución, a medida que la tecnología se vuelve omnipresente, las leyes y regulaciones necesarias nunca dejan de surgir. Un ejemplo simple es el caso de la reciente Ley de Divulgación de Seguridad Cibernética de 2017, un proyecto de ley estadounidense que propone tener informes periódicos obligatorios sobre experiencia en seguridad cibernética a nivel de directorio para empresas que cotizan en bolsa.

Es importante entender que la falta de adopción de medidas de seguridad razonables expone a una empresa no solo a los ciberdelincuentes, sino que también puede incurrir en

fuertes multas o sanciones por parte de los reguladores, juicios por negligencia y exposición mediática no deseada que puede afectar negativamente la imagen, marca y en última instancia, el valor de la empresa.

9.13 Programa de Auditoría interna.

OBSS INGENIERÍA tendrá un programa de Auditoria basado en la norma ISO 27001, la cual indica que se debe llevar auditorías internas para facilitar la información sobre el sistema de Gestión de seguridad de la Información (SGSI). [8]

El objeto también de llevar a cabo el plan o programa de auditoría interna se basa en la evaluación y capacidad para que los controles de la seguridad de la información que se establecieron en el diseño protejan los activos de información para OBSS INGENIERÍA. [8]

Para ello es importante que OBSS INGENIERÍA cumpla con los siguientes requisitos y que en base desde el diseño de la norma ISO27001, se debe garantizar para que quede registrado y documentado. [9]

A continuación, los requisitos.

- Planificar y mantener varios programas de auditoria donde se identifiquen los métodos y las responsabilidades de la elaboración del informe.
- Relevancia de los procesos implicados y los resultados de la auditoria.
- Los resultados de la auditoria se deben informar al área correspondiente de OBSS INGENIERÍA o directamente a la dirección.
- Definir el alcance de la auditoria y cual serán los criterios que se tendrán en cuenta.
- Guardar la información para que se utilice como evidencia cuando se lleve a cabo cualquier proceso evaluado.

10. Resultados

Como resultado del desarrollo de este trabajo obtenemos los siguientes entregables correspondientes a los requisitos mínimos para el diseño del sistema de gestión de la información los serán entregados a OBSS INGENIERÍA para poner en práctica las recomendaciones, políticas y estándares definidos en base a la norma iso 27001. OBSS INGENIERÍA dispondrá de la información con el objeto de implementar el sistema, fijar unos KPIs que le permitan a la organización iterar en los procesos, afinar detalles, perfeccionar las prácticas para acercar la realidad de la empresa a los lineamientos que define la norma y en un mediano plazo lograr la certificación de la norma ISO 27001.

10.1 Scope SGSI

Se entrega a OBSS INGENIERÍA un documento que detalla el alcance del SGSI para OBSS INGENIERÍA en la transmisión de datos de radios enlaces. Adicionalmente establece los requisitos mínimos para el diseño del SGSI, las recomendaciones y buenas prácticas que debe seguir la organización en base a la norma ISO 27001.

Ver Anexo 1_Alcance del SGSI.

10.2 Política y objetivos de la seguridad y privacidad de la información

En la definición de políticas de seguridad requeridas para la infraestructura, operación y servicios de OBSS INGENIERÍA se definió que la es sumamente importante documentar las políticas de seguridad que la organización requiere para la gestión de información, Posteriormente se pretende que OBSS INGENIERÍA ponga en práctica todas y cada una de las políticas con el fin de proteger su activo más valioso que es la información.

Siendo las políticas de seguridad una de las herramientas más importante en la gestión de la información se desarrolló un documento en el cual se consolidaron las políticas más relevantes aplicadas al modelo de negocio de OBSS INGENIERÍA. La aplicabilidad de las políticas estructuradas hará parte del plan de transformación de la organización en materia de seguridad, será un proceso de culturización que deberá hacer la paulatinamente con los usuarios, empleados, proveedores etc. o cualquier individuo que haga parte directa o indirecta en la gestión de la información.

Luego de la definición del alcance se identificó con la alta gerencia y con el acompañamiento técnico de la organización las políticas de seguridad que aplican en el desarrollo de las actividades de OBSS INGENIERÍA. Para la identificación de estás políticas se tuvo en cuenta la sede principal de la organización y el ciclo de procesos que llevan al interior para llevar a cabo la prestación de los servicios de radioenlaces.

Ver Anexo 2_Política de Seguridad y Privacidad.

Las políticas definidas hacen parte de la base de documentos iniciales que se proporcionaran a la organización con el fin de que se pueda poner en práctica cada una de las recomendaciones, este documento puede ser modificado por OBSS INGENIERÍA o tener control de cambios durante la etapa de afinamiento.

10.3 Metodología de evaluación del riesgo

Luego de la identificación de los riesgos en materia de seguridad de información de empresa OBSS INGENIERÍA se consolido en la información en una matriz, que permite detallar las causas, la frecuencia, los factores, controles y el impacto nivel de riesgo al que está expuesto la organización. En análisis se hallaron 12 riesgos los cuales fueron clasificados en técnicos, financieros, judiciales, operativos, ambientales y procedimentales su nivel de criticidad se determinó en función de la frecuencia, el impacto y los controles acorde con los siguientes criterios escalas de valoración como se muestra en las tablas:

DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
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 1 Tabla de Frecuencia.

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 presenta 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.

Tabla 2 Tabla de valoración de Controles.

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%

Tabla 3 Tabla de Valoración de Impacto

Luego de la clasificación de los riesgos, la guía 27005 sugiere detallar las causas generales y los efectos en los sistemas de información de la organización como se muestra en la siguiente tabla.

clasificación	Detalle del Riesgo	Causas Generales	Efectos
Técnicos	Indisponibilidad del servicio	* Ataque DoS * Robo de equipos de transmisión * fallas en los nodos *Virus en los sistemas informáticos * No contar con sistema de seguridad por capas	*Incumplimiento contractuales y de ANS de los servicios prestados a usuarios Finales.
Técnicos	filtración y hurto de información	* Acceso de personas no autorizadas en las áreas de trabajo. * No cifrar la información * No contar con licenciamientos requeridos para operar los servicios. * No bloquear puertos para la extracción de información * Contraseñas débiles * Ataques de fuerza bruta * Ataques de phising e ingeniería 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.
Técnicos	Acceso no autorizado a equipos de enrutamiento	* habilitación 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.
Financiero	Incumplimiento de ANS pacatdos con clientes	* Fallas en la red * Factores climáticos * No contar con redundancia de los servicios	*Indisponibilidad de Servicio *Incumplimiento a la meta de los servicios o ANS. *Multas contractuales.
Judicial	Interferencia en el espectro radioeléctrico 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.	* afectación de servicios a terceros * Multas por uso inadecuado de las frecuencias. * Deficiencias en la calidad de los servicios suministrado a usuario final.
Técnicos	Riesgo de Robo en los NODOS de TX.	Robo de equipos (facilites) 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.
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. *
Procedimental	Concepto de acto administrativo por parte de uno o varios colaboradores a favor de un tercero.	Beneficio económico a favor de un o varios colaboradores.	*Manipulación de información propia de OBSS. *Tráfico de influencias * Influencia de un tercero para obtener un concepto jurídico y/o acto administrativo a favor
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
Ambiental	Contaminación por residuos en Sitios Rurales o estaciones BASE.	NO contar con políticas de manejo de residuos eléctricos, químicos, 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.
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.
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. *incumplimiento de los ANS a usuario Final. *Penalizaciones por incumplimiento del servicio.

Tabla 4 identificación de los riesgos.

Luego de la determinación de las causas de los riesgos identificados se define el nivel de impacto inicial que presenta la organización de acuerdo con la cadena procesos que se ejecutan en OBSS INGENIERÍA.

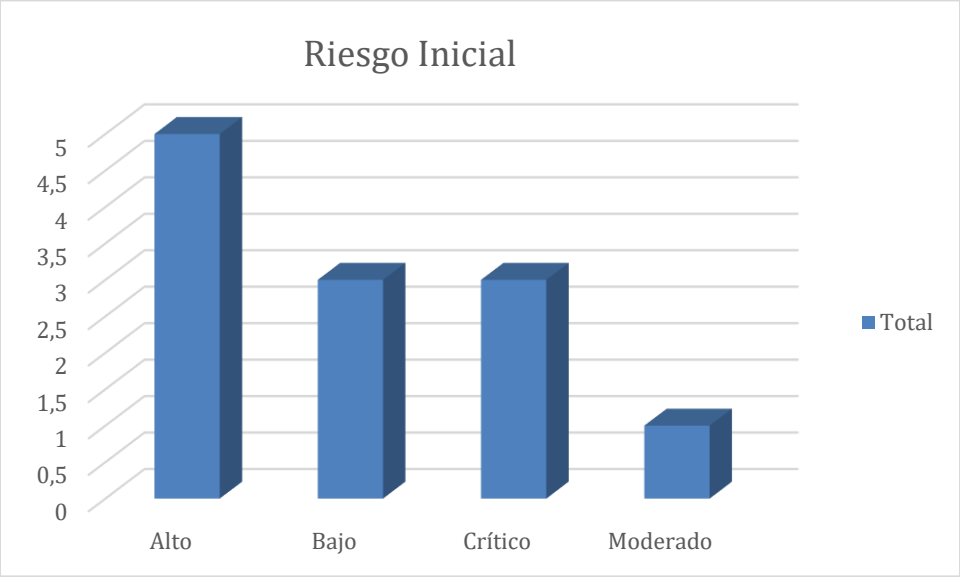

Tabla 5 Cantidad de Riesgos Iniciales identificados

En función de este análisis obtenemos un diagnóstico preliminar de organización en gestión de seguridad, los factores más críticos y pautas para definir el plan de tratamiento de los riegos.

El plan de tratamiento de riesgos fue estructurado en función de los controles necesarios a implementar y que hacen parte del plan de mitigación de los niveles de riesgos iniciales.

El riesgo objetivo contiene los planes de mejora que debe seguir OBSS INGENIERÍA en el desarrollo de las actividades a implementar, el presupuesto mínimo que se requiere a ejecutar en el plan de mejoramiento propuesto para OBSS INGENIERÍA y que hace parte del diseño del SGSI.

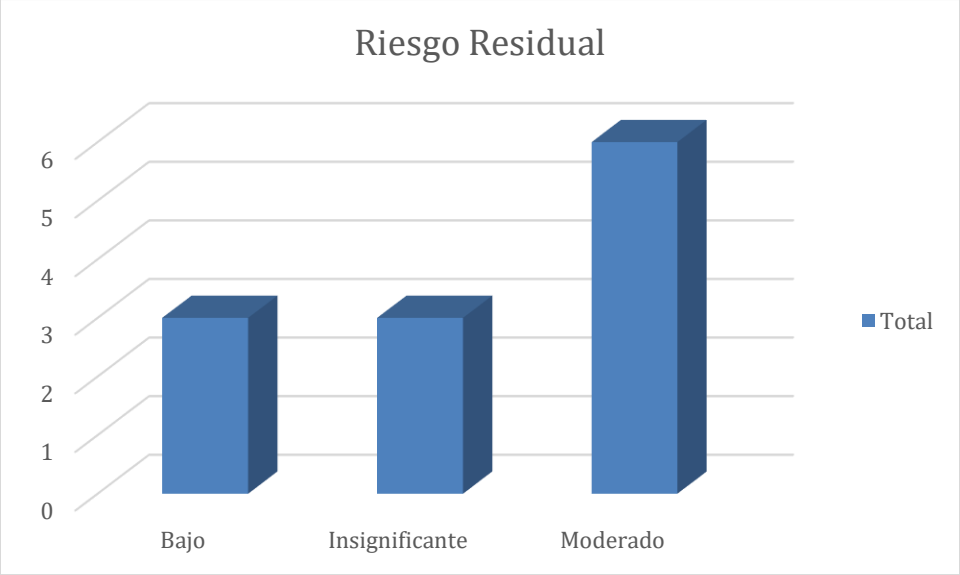

Tabla 6 Riesgos Residuales.

Ver Anexo 3_Matriz de Riesgos OBSS

10.4 Estado de aplicabilidad

El estado de aplicabilidad mostro el nivel de cumplimiento de la organización frente a los dominios y controles que sugiere el anexo A de la norma ISO 27001, en siguiente diagrama se registran los resultados luego de la valoración de cada uno de los controles, es evidente que la mayor cantidad no se cumplen en la organización, puntualmente 75 de los 114 controles los cuales corresponde a un 65 %, en donde 16 controles no aplican para los sistemas de información que dispone OBSS INGENIERÍA.

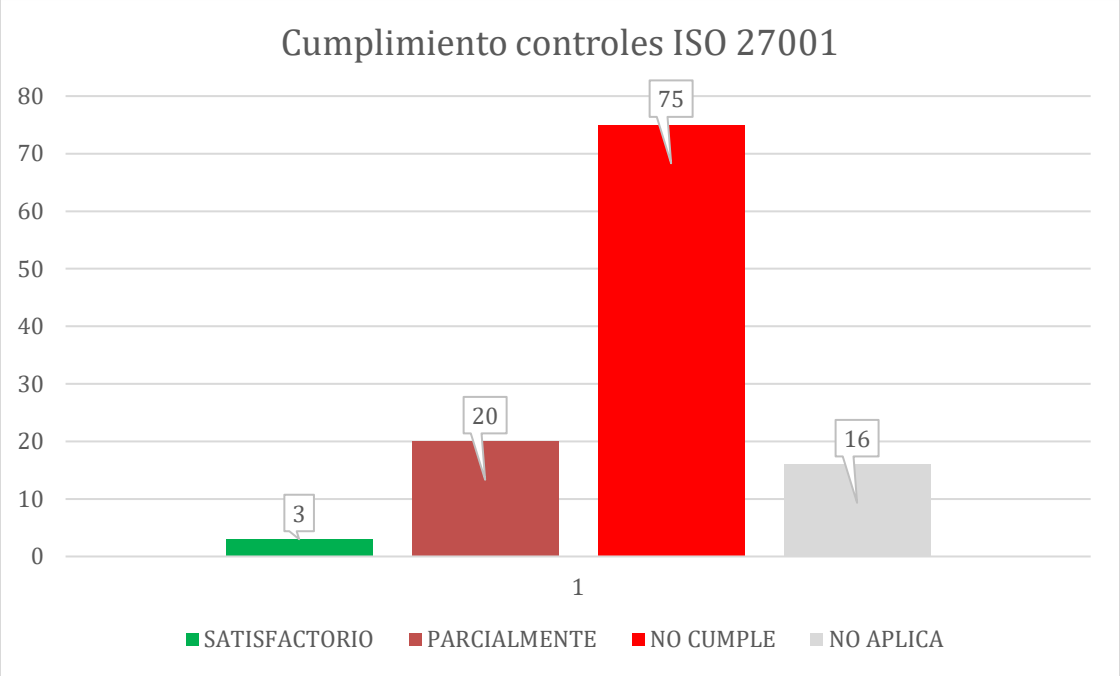

Tabla 7 Estado de Aplicabilidad OBSS INGENIERÍA.

Este análisis complementa la valoración de los riesgos y converge a la determinación del estado real de organización, establece las pautas y los puntos más críticos a los cuales la organización debe dar foco en la inmediatez posible para mitigar la materialización de los riesgos.

Ver Anexo 4_ Estado de Aplicabilidad OBSS

10.5 Plan de tratamiento del riesgo y presupuesto.

El plan de tratamiento del riesgo se construyó luego del análisis de criticidad y el estado de aplicabilidad de controles. Se obtuvo como resultado la definición de controles y el presupuesto por un valor de **COP 222.123.770** necesarios para adecuar la infraestructura y los procesos de gestión de información con el fin de adaptar y alinear la organización en la implementación de políticas y el uso de herramientas que le permitan asegurar dentro su actividad económica proteger su información frente a diversos tipos de ciberataques que directa o indirectamente está expuesto.

El presupuesto definido se calculó de acuerdo con las herramientas, equipos, procesos e infraestructura necesaria para mitigar los riesgos más críticos de la organización que comprometen la seguridad en la transmisión de información en los radioenlaces.

Solución	Ubicación	Cantidad	PRESUPUESTO	
			Opex	Capex
Firewall NGFW 600 E HA	Nodo principal	2		$ 45.997.770
CÁMARA TIPO BALA 1080P	Nodos	30		$ 750.000
Gabinete	Nodos	30		$ 600.000
NVR (4 canales)	Nodos	1		$ 633.000
Cámaras tipo domo	Nodo principal	15		$ 5.841.000
NVR (16) POE	Nodo principal	1		$ 13.890.000
Disco duro 1TB	Nodo principal	1		$ 302.000
Cable UPT (100 m)	Nodo principal	1		$ 256.000
Conector RJ45	Nodo principal	20		$ 100.000
Canaleta (100 m)	Nodo principal	1		$ 100.000
Rack (gabinete)	Nodo principal	1		$ 10.560.000
UPS (2 KVAs)	Nodo principal	31		$ 79.484.000
Cable HMI	Nodo principal	10		$ 50.000
pantallas de 43"	Nodo principal	5		$ 6.000.000
Servidor SSH	Nodo principal	1		$ 21.000.000
Servicios profesionales (50 horas)	Nodo principal	50	$ 7.500.000	
Canales alternos de internet10G	Nodo principal	2	$ 5.560.000	
Permisos Mintic uso espectro	Todos los nodos	1	$ 12.500.000	
Capacitaciones	Nodo principal	1	$ 5.000.000	
Tratamiento de residuos	Todos los nodos	1	$ 6.000.000	
TOTAL			$ 36.560.000	$ 185.563.770

Tabla 8 Presupuesto para plan de tratamiento del Riesgo.

Ver Anexo 3_ Matriz de Riesgos OBSS

10.6 Definición de roles y responsabilidades de seguridad

Como resultado obtenemos la estructuración de la matriz de roles y responsabilidades teniendo en cuenta la distribución de los recursos actuales con el que dispone OBSS INGENIERÍA y los que se requiere como recomendación de la norma para asegurar en las actividades un desempeño correcto a nivel de responsabilidad en todos los factores que pueden afectar o poner en riesgo la seguridad de la información.

Los roles son aprobados por la alta gerencia de OBSS INGENIERÍA, se da el entendimiento y el alcance de cada uno frente al desarrollo de las actividades dentro de la organización, se consolida la información en el documento entregable y se formaliza un acta con los compromisos que debe adoptar rol.

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

Tabla 9 Tabla Matriz de Roles y Responsabilidades

Ver Anexo 5_ Matriz de roles y Responsabilidades.

10.7 Inventario de activos

Además de consolidar la cantidad de activos de información que posee OBSS INGENIERÍA, este análisis permitió detallar cuales son vulnerabilidades, amenazas y el impacto que puede tener la confidencialidad, la integridad y la disponibilidad de la información de OBSS INGENIERÍA.

En base a la metodología de la guía ISO 27005 se identifican los activos de la organización, y se agrupan de acuerdo con la siguiente clasificación:

- HARDWARE
- SOFTWARE
- REDES
- LUGAR
- PERSONAL

Clasificación del Activo	Activo de información
HARDWARE	Router de Borde
	Router distribución
	Router agregación
	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)
	Ofimática (servidor)
	Correo (como Hosting)
	Documentos en Drive
	Software para línea de vista - Mikrotic - Cambium
REDES	WAN
	LAN
	Enlaces 2GB (banda milimétrica 60 y 80 GHz)

	Rack
	Enlaces 1GB (banda licenciada 11 GHz)
LUGAR	Predios
PERSONAL	Gerencia administrativa
	Ejecutivo comercial senior
	Ejecutivo comercial junior
	Revisor fiscal
	Contador
	Arquitecto redes
	Jefe técnico
	Técnicos de redes

Tabla 10 Activos Identificados en el proceso de Transmisión de Radioenlaces.

Posteriormente se realiza la identificación de las vulnerabilidades, amenazas y cual sería el impacto de acuerdo con las causas representando la probabilidad de ocurrencia y la consecuencia de la ocurrencia, para la valoración del impacto se desarrolló de acuerdo con los niveles y escalas definidas en la siguiente tabla:

		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

Tabla 11 Matriz de Impacto sobre los Activos de Información.

A continuación, se detalla en la siguiente gráfica los niveles de impacto para cada uno de los activos identificados en el servicio de radioenlaces de OBSS INGENIERÍA. Por lo que se puede observar que el 92% de la totalidad de los equipos representa un nivel de impacto Extremo, esto significa que se puede ver comprometida la transmisión, procesamiento y almacenamiento de la información.

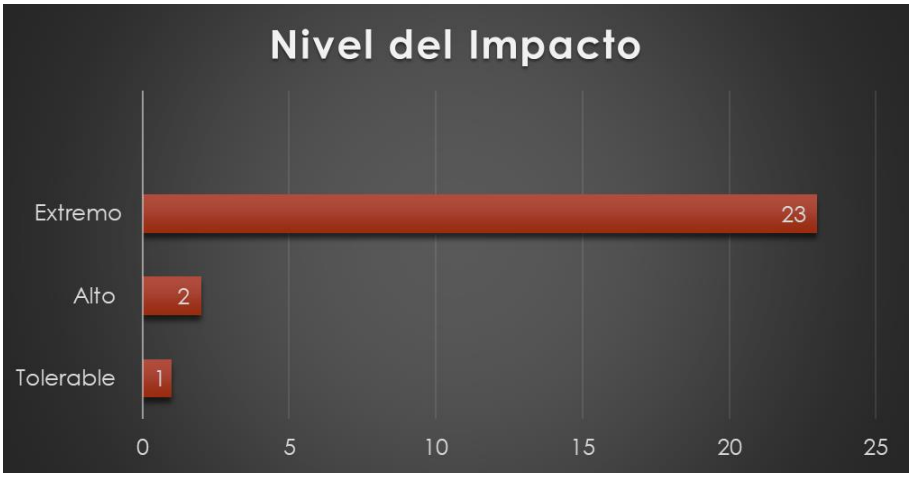

Ilustración 3 Nivel de impacto en los Activos.

Ver Anexo 6_ Inventario de Activos.

10.8 Política de seguridad de Proveedores

El objetivo de esta política de gestión de proveedores busca 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.

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.

Se entrega a OBSS INGENIERÍA un documento base con dos escalas de controles que dan cumplimiento a la política de seguridad en relación con los proveedores1

- **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.

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.

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

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 12 Controles Política de Seguridad de Proveedores.

Ver Anexo 7_ Relación de Proveedores.

10.10 Procesos de gestión de incidentes

Para los procesos de gestión de incidentes se establece una prioridad en función de su clasificación de severidad, como resultado obtenemos la siguiente tabla que consolida el nivel a que corresponde, de manera que los niveles de atención tengan una herramienta para clasificar inicialmente la criticidad de un incidente y establecer como una prioridad para la resolución de esta.

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

Tabla 13 matriz de clasificación de Incidentes.

Se definen 3 niveles de atención para la gestión de incidentes los cuales procederán bajo las casuísticas y criterios definidos en cada caso, adicionalmente se construye una matriz con los tiempos máximo de atención según la ubicación de los servicios de OBSS INGENIERÍA.

Dentro del proceso de gestión de incidentes se define el responsable en cada uno de los niveles de atención acorde con la matriz de roles y responsabilidades definidas para la organización.

Ver Anexo 8_ Política de Gestión de Incidentes.

10.11 Proceso de continuidad del negocio

Como se puede observar en la ilustración, 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 implementación del SGSI y desde el diseño asegurará que la empresa pueda llevar a cabo planes que garanticen como entrar el servicio en el menor tiempo posible y cómo reaccionar ante este tipo de eventos.

Ilustración 4 Continuidad del Negocio_Fuente: MINTIC

Ver Anexo 9_ Plan de continuidad del Negocio.

Se entrega un documento a OBSS INGENIERÍA, donde se especifica el objetivo, la gestión de la continuidad del negocio y el análisis del impacto del negocio, partiendo desde el diseño del SGSI para la organización, teniendo en cuenta que 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 dé 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.

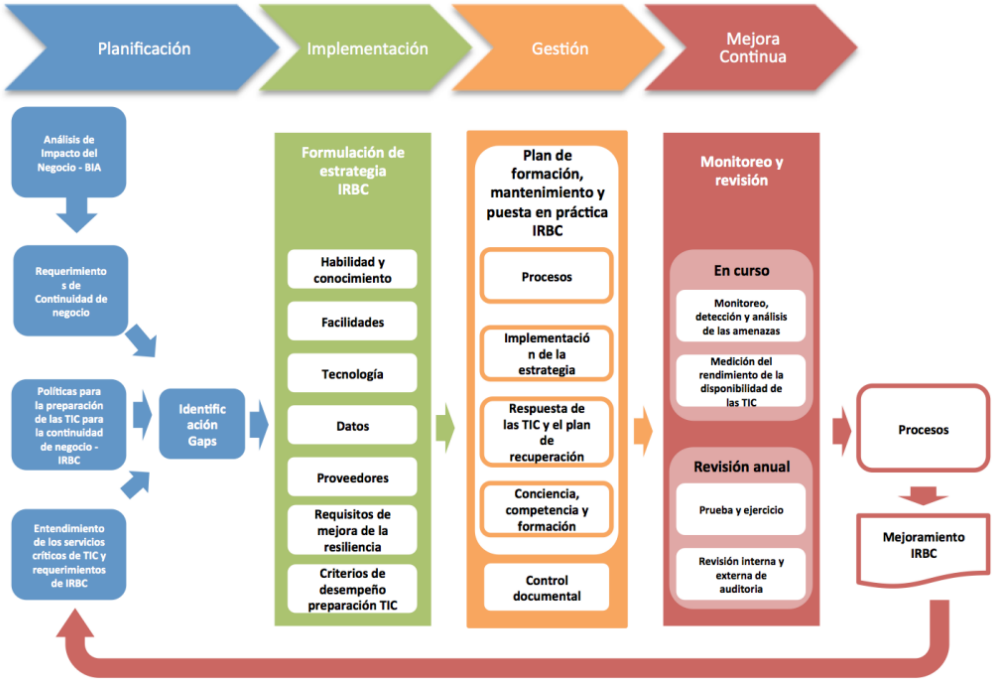

Ilustración 5 Marco de Continuidad del Negocio para la seguridad y privacidad de la información. Fuente MINTIC.

10.12 Normograma.

Se consolidan todos los lineamientos legales, normativos, regulatorios y decretos que debe cumplir OBSS INGENIERÍA en el ejercicio propio de las actividades del negocio, entiendo que bajo su incumpliendo estará sujeto a procesos jurídicos que podría significar una sanción a la organización. Por lo anterior se hace necesario tener claro y documentado los reglas a las se debe acoger:

- Resolución 1075 de 2020
- Resolución 1588 de 2012
- Resolución 2118 de 2011
- Resolución 917 de 2015
- Resolución 83 de 2008 Ministerio de Comunicaciones
- Resolución 970 de 2011
- Decreto 4392 del 23 de noviembre de 2010
- Decreto 1161 de 2010 Nivel Nacional
- Decreto 4392 de 2010 Nivel Nacional
- Decreto 2044 de 2013 Nivel Nacional
- Decreto 542 de 2014 Nivel Nacional
- Decreto Único Reglamentario 1078 de 2015 Nivel Nacional
- Decreto 984 de 2022 Nivel Nacional
- Ley 1341 de 2009 Nivel Nacional
- Ley 1753 de 2015 Nivel Nacional
- Ley 1978 de 2019 Congreso de la República de Colombia"
- Circular No. 01 de 2021

- Norma ISO 27001
- Norma ISO 27006
- Norma ISO 27009

[10]

En el proceso de implementación del SGSI el entregable podrá surtir algunos cambios entono a las iteraciones y las actualizaciones en material legal que se pueda generar dentro de la operación de transmisión de Datos por medio de Radioenlaces.

Ver Anexo 10_ Normograma.

10.13 Procedimiento de Auditoria.

Para el plan o programa de auditoría externa se detalla los lineamientos y cuáles son los pasos para seguir para OBBS INGENIERÍA; una vez, se encuentren en la capacidad de la implementación del SGSI basado en la norma ISO 27001:2013, pues el programa de auditoria se rige cuando se tiene implementado el SGSI.2

Adicionalmente se detalla los procesos que se deben aplicar trimestral para auditar el cumplimiento de estos en la organización, es importante notar que, aunque es parte de los lineamientos de la fase de diseño, se establece dentro del documento un formato inicial que OBSS INGENIERÍA podrá usar y ajustar una vez realice la respectiva implementación del SGSI.

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

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

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

2. ALCANCE	
EXCLUSIONES	

3. DEFINICIONES

1. OBJETIVOS

2. RESULTADOS

6. Observaciones y Oportunidades de Mejora

3. CONCLUSIONES

Tabla 14 Documento base para control de Auditoria trimestral.

El formato de la table No 15, es una base que se propone a la organización para llevar el control trimestral del plan de auditoría. OBSS INGENIERÍA podrá realizar modificaciones o cambios de este de acuerdo con el plan de implementación del SGSI realizado.

Ver Anexo 11_ Procedimiento de Auditoria.

11. Cronograma.

El cronograma propuesto para la implementación del SGSI basado en la Norma de la ISO 27001-2013, se proyectó de acuerdo con las actividades y tareas que va a ejecutar OBSS INGENIERÍA de acuerdo con los formatos y documentos sugeridos en la etapa de diseño. Es importante aclarar que este cronograma puede tener variaciones en función de lo que establezca la organización y en la medida que se tengan aprobaciones de los recursos tanto financieros como técnicos.

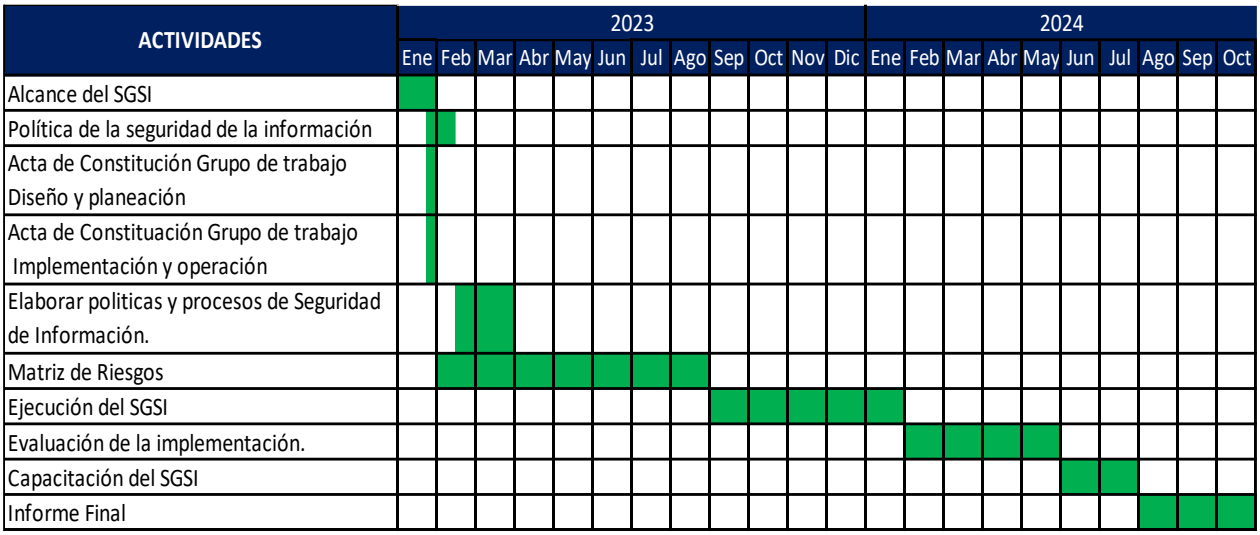

Ilustración 6 Cronograma propuesto para la implementación del SGSI.

12. Discusión.

Si bien el diseño presentado contiene los requisitos mínimos para la certificación en norma ISO 27001, OBSS INGENIERÍA deberá realizar la implementación del sistema, capacitar a sus empleados, poner en práctica cada una de las políticas y procesos estructurados a fin de llevar la organización a un grado mayor de madurez a nivel de seguridad de información.

La implementación del SGSI es un proceso iterativo incremental hasta lograr un equilibrio en la organización, es una transformación que debe lograr en toda la organización a fin de obtener el conocimiento, la responsabilidad y la experiencia frente a la seguridad de la información, por lo anterior recomendamos a la OBSS INGENIERÍA iniciar este proceso bajo el acompañamiento de un profesional experto en la norma.

La documentación entregada a OBSS INGENIERÍA es un paso importante dentro del camino que debe recorrer para lograr la certificación, sin embargo para alcanzar este objetivo la organización debe empezar por la culturización de la seguridad de la información en todos los frentes, la seguridad es responsabilidad de todos los miembros, su efectividad depende de la claridad de las políticas y procesos, no solamente del área de TI es el responsable de la seguridad, en muchas empresas se cae en este error. En la medida en que se ponga en práctica todas las recomendaciones consolidadas en este documento, se podrán generar modificaciones en base a los resultados de aplicabilidad no es una camisa de fuerza la información entregada, OBSS INGENIERÍA podrá ajustar y afinar la información en la dinámica de la implementación.

13. Conclusiones

Se realizo un diagnóstico preliminar del estado de la seguridad de la información con el análisis de riesgos, clasificación de activos y estado de aplicabilidad. Bajo este análisis fue posible conocer a detalle los riegos, vulnerabilidades y amenazas a los que está expuesto la organización, dicha información se convirtió en el punto de partida para construir los planes de mejora, las políticas y los procesos que recomienda la norma frente a la gestión de la información.

Se estructuro un diseño de un SGSI para todos los procesos y actividades referentes a la transmisión de datos sobre radio enlaces de la empresa OBSS INGENIERÍA. El diseño contempla los requisitos mínimos requeridos para la certificación de norma ISO 27001, con la documentación correspondiente para que OBSS INGENIERÍA inicie su implementación.

Se construyó un plan de tratamiento del riesgo, basando en controles de seguridad para cada uno de los riesgos identificados, de esta forma se determinó las herramientas y presupuesto que requiere la organización para asegurar los controles correspondientes sobre la infraestructura y el recurso humano a fin de lograr la disponibilidad, integridad y confidencialidad de la información.

Se documento toda la información necesaria para el cumplimiento de los requisitos mínimos de la certificación de la norma ISO 27001, sin embargo, OBSS INGENIERÍA debe poner en práctica las recomendaciones, implementar es el SGSI, ajustar en función de los resultados y llevar la organización a un plan de mejora continua. La documentación entregada no es definitiva, en la medida de la aplicación de las políticas y procesos se buscará la estandarización y simplificación de los procesos desde cada una de las áreas que participan en la gestión de la información, adicionalmente OBSS INGENIERÍA deberá actualizarse constantemente a las variaciones de la norma y la dinámica del ciber entorno.

14. Bibliografía

[1] ISO 27001, «Diseñando un SGSI,» 04 05 2019. [En línea]. Available: https://normaiso27001.es/fase-6-implementando-un-sgsi/.

[2] 27001 academy, «White paper: Checklist of Mandatory,» 02 09 2014. [En línea]. Available: https://advisera.com/27001academy/wp-content/uploads/sites/5/2015/06/Checklist_of_ISO_27001_Mandatory_Documentation_EN.pdf.

[3] Mango, «Mango Live,» 15 07 2021. [En línea]. Available: https://www.mangolive.com/information-security-policy-and-objectives.

[4] ISOTools, «ISO 27001: Evaluación y tratamiento de riesgos en 6 pasos,» 30 05 2021. [En línea]. Available: https://www.isotools.com.co/iso-27001-evaluacion-tratamiento-riesgos-6-pasos/.

[5] ANI, «Plan de Tratamiento de riesgos de la seguridad digital,» 30 01 2022. [En línea]. Available: https://www.ani.gov.co/sites/default/files/plan_de_tratamiento_de_riesos_de_seguridad_de_la_informacion_v5_15-4-2020.pdf.

[6] DataGuard, «ISO 27001 Risk Treatment Plan: How to develop the right one,» 18 04 2020. [En línea]. Available: https://www.dataguard.co.uk/blog/iso-27001-risk-treatment-plan-what-you-need-to-know#one.

[7] Austalian Government , «ISO 27001 Risk assessment and,» 15 05 2022. [En línea]. Available: file:///C:/Users/hafac/Downloads/20220502%20ISO%2027001%20risk%20assessment.pdf.

[8] ISOToolS, «Seguridad de la Información,» 11 04 2019. [En línea]. Available: https://www.pmg-ssi.com/norma-27001/9-2-auditoria-interna/.

[9] Universidad Tecnológica de Pereira, «GESTIÓN DEL SISTEMA INTEGRAL DE CALIDAD,» 25 06 2021. [En línea]. Available: https://www.sinergiasempresariales.com/auditoria-iso-27001/.

[10] Jurisdicción Especial para la PAZ, «Normatividad,» 05 10 2022. [En línea]. Available: https://www.jep.gov.co/Normativa/Paginas/Normograma.aspx.

[11] MINISTERIO DE LAS TIC, «Guía para la preparación de las TIC,» 15 12 2010. [En línea]. Available: https://www.mintic.gov.co/gestionti/615/articles-5482_G10_Continuidad_Negocio.pdf.

15. Anexos

Se adjuntan con este documento los siguientes anexos: