

**DISEÑO DE UNA PROPUESTA METODOLÓGICA PARA LA GESTIÓN DE LA
SEGURIDAD DE LA INFORMACIÓN EN LA INFRAESTRUCTURA TECNOLÓGICA
EN EL CABILDO INDÍGENA RESGUARDO DE JAMBALÓ.**

AUTOR

JERSON RONALDO MARTINEZ TROCHEZ

CORPORACION UNIVERSITARIA COMFACAUCA UNICOMFACAUCA

INGENIERÍA DE SISTEMAS

PROYECTO DE GRADO

SANTANDER DE QUILICHAO

2025

**DISEÑO DE UNA PROPUESTA METODOLÓGICA PARA LA GESTIÓN DE LA
SEGURIDAD DE LA INFORMACIÓN EN LA INFRAESTRUCTURA TECNOLÓGICA
EN EL CABILDO INDÍGENA RESGUARDO DE JAMBALÓ.**

AUTOR:

JERSON RONALDO MARTINEZ TROCHEZ

**PROYECTO DE GRADO PARA OPTAR EL TÍTULO DE INGENIERÍA DE
SISTEMAS**

DIRECTOR OPCIÓN DE GRADO:

TORRES BERMÚDEZ ALEX ARMANDO

CORPORACION UNIVERSITARIA COMFACAUCA UNICOMFACAUCA

INGENIERÍA DE SISTEMAS

Nota de Aceptación

.....

Presidente del Jurado

.....

Jurado

.....

Jurado

Ciudad y Fecha (día, mes, año) (Fecha de entrega)

AGRADECIMIENTOS

Principalmente quiero dar gracias a Dios por todas las bendiciones que me ha brindado, a mi madre Arcelia Trochez que me dio la vida y a mi padre Osnoraldo Martinez, que con muchos sacrificios me ayudaron a terminar el proceso de formación, a mi hijo Daniel Sebastián Martinez Dagua quien es mi esperanza y mi motivo de superación de vida, a la Corporación Universitaria ComfacaUCA UnicomfacaUCA y a sus docentes que me guiaron en este proceso, por el compromiso y dirección con sus conocimientos y a todos mis compañeros de grado que estuvieron en cada uno de mis procesos.

Contenido

RESUMEN.....	12
INTRODUCCIÓN.....	13
CAPÍTULO 1.....	15
1. PLANTEAMIENTO Y DESCRIPCIÓN	15
1.1. FORMULACIÓN DEL PROBLEMA.....	17
1.2. JUSTIFICACIÓN	18
1.3. OBJETIVOS.....	21
1.3.1. Objetivos General:	21
1.3.2. Objetivo Específicos:.....	21
1.4. MARCO TEÓRICO	22
1.4.1. La seguridad de la información como pilar organizacional	22
1.4.2. Sistema de Gestión de Seguridad de la Información	23
1.4.3. Norma ISO/IEC 27001 2022: y el Sistema de Gestión de Seguridad de la	
Información	24
1.4.4. Norma ISO 31000:2018 y la cultura de gestión del riesgo	25
1.4.5. Aplicación de las normas en contextos comunitarios.....	25
1.4.6. Seguridad informática	26
1.4.7. Políticas de seguridad informática	28
1.4.8. Controles de seguridad	30

1.4.9.	Modelo PHVA aplicado a los procesos SGSI	31
1.5.	MARCO LEGAL:	33
1.6.	Normativas, estándares y buenas prácticas internacionales en gestión de la seguridad de la información aplicables al contexto en el Cabildo Indígena resguardo de Jambaló.	34
CAPITULO 2.....		36
2.	METODOLOGÍA	36
2.1.	INSTRUMENTOS PARA LA RECOLECCION DE INFORMACION ...	36
2.2.	FASES METODOLÓGICAS	37
CAPÍTULO 3.....		38
3.	DISEÑO UNA PROPUESTA METODOLÓGICA PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN LA INFRAESTRUCTURA TECNOLÓGICA EN EL CABILDO INDÍGENA RESGUARDO DE JAMBALÓ.....	38
3.1.	El alcance y límites del proyecto	38
3.2.	Fase 1- Diagnostico del estado actual de la infraestructura tecnológica y de la gestión de la seguridad de la información en el Cabildo Indígena del Resguardo de Jambaló:	39
3.2.1.	Evidencia de campo	40
3.2.2.	Encuesta	41
3.3.	Fase 2 – Contexto organizacional	44
3.3.1.	Naturaleza del cabildo indígena resguardo Jambaló.....	44

3.3.2. Surgimiento del plan de vida proyecto global.....	46
3.3.3. ESTRUCTURA ORGANIZACIONAL	48
3.4. Fase 3 Planificación del SGSI	52
3.4.1. Tipos de activos.....	53
3.4.2. Identificación de los activos	54
3.4.3. Criterios de fundamentales para la clasificación de activos	56
3.4.4. Nivel de criticidad de los activos de la organización.....	57
3.4.5. Valoración de Riesgos de seguridad	58
3.4.5.1. Identificación de riesgos de seguridad	59
3.4.5.3. Identificación de Amenazas.....	60
3.4.5.4. Identificación de Vulnerabilidades.....	61
3.4.5.5. Análisis y evaluación del Impacto riesgo:	61
3.4.5.6. Evaluación de la Probabilidad	62
3.4.5.7. Cálculo del Riesgo	63
3.5. POLÍTICAS DE SEGURIDAD	64
3.5.1. Políticas de seguridad de la informacion asociado al control de seguridad	69
3.5.2. Análisis y evaluación del Impacto riesgo:	70
3.5.3. Evaluación de la Probabilidad.....	71
3.5.4. Clasificación de evaluación de riesgo	71

3.5.5. Plan de tratamiento de Riesgos.....	71
3.5.5.1. Estimación de un presupuesto global	73
CAPÍTULO 4.....	74
4. RESULTADOS ALCANZADOS	74
4.1. Identificación e inventario de activos	75
4.2. Plan de tratamiento riesgo	75
4.3. Evaluación de la Probabilidad	78
4.4. Nivel de riesgo.....	78
4.5. Mapa residual de riesgo	78
4.6. Contingencia de control de seguridad	79
4.7. Mitigación y mejoras resultados diseño una propuesta metodológica para la gestión de la seguridad de la información en la infraestructura tecnológica en el cabildo indígena resguardo de Jambalo.	81
4.8. Diseño y presentación de la propuesta del sistema de gestión de seguridad a la Autoridades ancestrales	82
4.9. Certificación y aval de la implementación del sistema de gestión de seguridad.	82
CAPÍTULO 5.....	83
5. CONCLUSIONES.....	83
5.1. Trabajos a futuro	84
BIBLIOGRAFÍA	85

ANEXOS.....89

LISTA DE FIGURAS

Figura 1 Sistema de gestión de seguridad	23
Figura 2 Norma ISO 27001 POR ESTEBAN SAN ROMAN CYNTHUS	30
Figura 3 Ciclo PHVA en un SGSI	32
Figura 4 Estructura organizacional	48
Figura 5 Piso Área administrativas	92
Figura 6 2 Piso Autoridades Ancestrales.....	93
Figura 7 3 Piso Representante Legal	93
Figura 8 2 piso Núcleo de Educación	94
Figura 9 3 Piso Núcleo de Educación.....	95
Figura 10 Emisora Comunitaria	96

LISTA DE TABLAS

Tabla 1 Tipos de Activos	53
Tabla 2 Identificación de activos.....	54
Tabla 3 activos	55
Tabla 4 Nivel de criticidad de activos	57
Tabla 5 Valoración de criticidad de activos.....	58
Tabla 6 Identificación de amenazas	60
Tabla 7 Identificación de vulnerabilidades	61
Tabla 8 Analisis y evaluación de riesgo.....	62
Tabla 9 Probabilidad de riesgo	62
Tabla 10 Calculo de riesgo.....	63
Tabla 11 Norma ISO 27001.....	64
Tabla 12 Resumen políticas de seguridad	68

RESUMEN

El Cabildo Indígena Resguardo de Jambaló, Cauca, es una entidad pública de carácter especial, sin ánimo de lucro y legalmente constituida por el Ministerio del Interior. Su estructura político-organizativa se fundamenta en la ley de origen y el derecho mayor, lo que le otorga autonomía en la gestión de sus procesos comunitarios. surge la necesidad un diseño de gestión de seguridad de la información que permitan proteger los activos tecnológicos e información sensible de la organización, debido a las crecientes amenazas y vulnerabilidades a las que se encuentra expuesta.

El presente proyecto tiene como propósito abordar la gestión de seguridad de la información, tomando como referencia las normas internacionales ISO 27001 e ISO 31000. con el propósito de salvaguardar los activos de información y protegerlos frente a amenazas y vulnerabilidades. A partir de un estudio de campo, se identificó la ausencia de lineamientos claros en materia de seguridad, lo que representa una debilidad organizacional significativa lo cual comprometen la confidencialidad, integridad y disponibilidad de la información.

La propuesta busca fortalecer la protección de los activos de información del Cabildo, evidenciando la aplicabilidad y pertinencia de estándares internacionales en contextos comunitarios, culturales y geográficos particulares, contribuyendo así al desarrollo organizacional y a la sostenibilidad en la gestión de la información.

INTRODUCCIÓN

La protección de la información constituye en la actualidad una prioridad para todas las organizaciones, sin importar su naturaleza o tamaño, debido a la constante exposición a amenazas tecnológicas que ponen en riesgo la confidencialidad, integridad y disponibilidad de los datos (ISO, 2022). Ante este panorama, el presente proyecto se enfoca en la gestión de la seguridad de la información en la infraestructura tecnológica del Cabildo Indígena Resguardo de Jambaló, con el propósito de salvaguardar sus recursos tecnológicos, reducir riesgos y aplicar buenas prácticas orientadas a la prevención de incidentes.

En este contexto, surge la necesidad de abordar de manera formal y estructurada la problemática de la seguridad de la información dentro de la organización indígena. La falta de lineamientos y políticas claras en materia de gestión de riesgos expone a la comunidad a posibles amenazas y vulnerabilidades que no solo podrían comprometer la confidencialidad e integridad de los datos, sino también afectar la continuidad de sus operaciones tecnológicas y administrativas.

El documento se organiza en cinco capítulos. En los cuales describe el proceso planteado a lo largo del proyecto:

El **Capítulo 1** describe el problema actual del Cabildo e integra los conceptos teóricos de referencia.

El **Capítulo 2** presenta la metodología de investigación, fundamentada en las normas ISO/IEC 27001:2022 e ISO 31000, y apoyada en un enfoque de investigación de campo para identificar riesgos y analizar sus causas.

El **Capítulo 3** desarrolla la propuesta metodológica mediante un diagnóstico preliminar, la formulación de políticas y la definición de controles de seguridad.

El **Capítulo 4** expone los resultados alcanzados, entre ellos la identificación e inventario de activos, el plan de tratamiento de riesgos y las medidas de contingencia. Finalmente, el **Capítulo 5** resalta la importancia que tiene los sistemas de gestión de la seguridad de la información en organizaciones comunitarias e institucionales.

CAPÍTULO 1

1. PLANTEAMIENTO Y DESCRIPCIÓN

Hoy en día los sistemas de gestión de seguridad de la información en todas las organizaciones son de carácter fundamental, es por ello que es necesario salvaguardar la información sensible de los diferentes amenazas y vulnerabilidades latentes en la organización.

Según informes por la fiscalía general de la nación en el 2021 aumento los ataques cibernéticos a entidades del gobierno a 30% comparado con el año anterior, lo cual es necesario que todas las organizaciones busquen estrategias para salvaguardar la informacion.

Además, las comunidades indígenas en la era digital, han experimentado un aumento significativo en la dependencia de la tecnología y el manejo de la información. Esta evolución tecnológica ha aportado beneficios a la comunidad dentro de los que se identifican el ahorro de tiempo de respuesta, ejecución de procesos más eficientes y posibilidad de implementar nuevos procesos en términos de comunicación, acceso a recursos y desarrollo, pero también ha introducido nuevos desafíos en cuanto a la seguridad de la información y la preservación de la identidad cultural.

OSPINA DIAZ, Milton Ricardo y SANABRIA RANGEL, Pedro Emilio. Aborda los desafíos que enfrenta colombia en materia ciberseguridad dentro del contexto global, plantean que los sistemas de informacion, la internet y la computadora en la nube constituyen un soporte fundamental para el almacenamiento, gestión y aplicación de información personal y organizacional, lo cual los convierte en un blanco para quienes quieren robar, manipular o dañar, o desean afectar a sus propietarios.

En este contexto, surge la necesidad de abordar el problema de la seguridad de la información en la infraestructura tecnológica del Cabildo Indígena Resguardo de Jambaló. La falta de un enfoque formal y estructurado para gestionar los riesgos de seguridad de la información que expone a la comunidad a posibles amenazas y vulnerabilidades que podrían comprometer tanto la confidencialidad como la integridad de los datos, así como afectar la continuidad de las operaciones tecnológicas.

El desafío se agrava en la organización debido a la falta de directrices y estrategias claras de políticas de seguridad y controles de seguridad adecuados de un modelo que permita establecer, implementar, monitorear, revisar y mantener la protección de la información en el contexto específico de una comunidad indígena.

Actualmente el Cabildo Indígena Resguardo de Jambaló almacena un volumen considerable de información en sus bases de datos y dispositivos tecnológicos, los cuales, están expuestos a vulnerabilidades, además la creciente dependencia de sistemas y dispositivos electrónicos, así como el manejo de datos digitales, ha expuesto a la comunidad a una serie de riesgos de seguridad de la información.

Estos riesgos pueden manifestarse en forma de ciberataques, accesos no autorizados a datos sensibles, pérdida de información crítica debido a fallas tecnológicas y más. Dada la naturaleza única del Cabildo Indígena Resguardo de Jambaló donde buscan la preservación cultural, la pérdida o alteración de datos y la interrupción de las operaciones tecnológicas podrían tener consecuencias especialmente significativas.

A pesar de esta situación, hasta la fecha no se ha implementado un sistema formal para abordar estos riesgos y establecer una cultura sólida de seguridad de la información. La ausencia

de políticas, procedimientos y controles específicos en esta área deja a la comunidad vulnerable a amenazas y vulnerabilidades que podrían ser mitigadas mediante la adopción de un enfoque más estructurado.

Vergara Torres, O.H. (2019) resalta que la aplicabilidad de la seguridad de la información es responsabilidad de las organizaciones, así como la protección de los datos y el mantenimiento de la confidencialidad.

La norma ISO 27001: 2022 proporciona un marco reconocido internacionalmente para la implementación de un Sistema de Gestión de Seguridad de la Información. Sin embargo, su adaptación y aplicación directa a la realidad y necesidades del Cabildo Indígena Resguardo de Jambaló requerirá una evaluación minuciosa y personalizada de los riesgos y controles adecuados.

Por lo tanto, el problema que se aborda en este proyecto está relacionado con la Gestión de Seguridad de la Información con el fin de que sea pertinente, efectivo y acorde con la infraestructura tecnológica del Cabildo Indígena Resguardo de Jambaló. La solución a esta problemática permitirá proteger la información sensible, salvaguardar los activos tecnológicos y contribuir a la identidad cultural de la comunidad en un entorno digital.

1.1. FORMULACIÓN DEL PROBLEMA

¿Cómo contribuye la validación de una propuesta metodológica para la Gestión de la Seguridad de la Información en la infraestructura tecnológica en el cabildo indígena resguardo de jambaló en mejora de la protección de los datos?

1.2. JUSTIFICACIÓN

En Colombia y en el mundo se han incrementado los ataques informáticos a organizaciones o empresas además se ha convertido en una prioridad de todos los tamaños, gracias a la evolución de la tecnología y de los sistemas de información, todas las organizaciones se expone a diferentes amenazas latentes, cada año surgen nuevas amenazas, es primordial estar al tanto de las nuevas tendencias y de los riesgos potenciales para proteger adecuadamente los sistemas, lo cual radica en la necesidad urgente de garantizar la seguridad de la información en la infraestructura tecnológica del Cabildo Indígena Resguardo de Jambaló, que permita identificar y mitigar estas amenazas, fortaleciendo la resiliencia ante posibles ataques.

Según el ultimo informe del centro cibernético de la policía nacional al cierre del 2024 en colombia aumento un 23% en denuncias cibernéticas las ciudades con mayor caso fueron Bogotá, Medellín y Cali, los incidentes más frecuentes fueron acceso abusivo al sistema de informacion, violación de datos personales, phishing y malware.

El Cabildo Indígena Resguardo de Jambaló es una organización indígena con una estructura política administrativa que a lo largo del tiempo ha permitido avanzar en los proyectos comunitarios orientados desde las asambleas con el propósito de avanzar en el desarrollo educativo, económico, salud y gobierno propio. Fue creado en el año 1986 donde los procesos comunitarios se han transformado en procesos tecnológicos.

El cabildo indígena resguardo de jambalo maneja sistemas de información, como cuéntame que es una base de datos que utiliza la organización para el manejo de información de los niños ante el bienestar familiar ICBF, de igual manera utiliza bases de datos para el censo de la comunidad que maneja ante el gobierno y dispositivos tecnológicos que utilizan para gestionar

los procesos de índole territorial esto conlleva a la necesidad de un sistemas de gestión de la seguridad de información que permita proteger la integridad de la información.

Ningún tipo de organización o empresa esta exacta de recibir amenazas cibernéticas por ejemplo la empresa la EPM “EMPRESAS PUBLICAS DE MEDELLIN en el 2022 fue víctima de un ransomware que cifro alrededor de 25% de los servidores, incluyendo sistemas de facturación y atención al cliente.

Según Forbes Colombia. De acuerdo con ese informe, por segundo año consecutivo, Colombia se ha convertido en el país más atacado por ataques cibernéticos, con el 17% de los incidentes en la región.

En un mundo cada vez más digitalizado, donde las tecnologías y los datos desempeñan un papel fundamental en todas las esferas de la sociedad, es crucial abordar de manera proactiva los riesgos de seguridad asociados con la gestión de información, además la adopción de tecnología conlleva nuevos riesgos, incluidos ciberataques, piratería informática y robo de datos. La falta de medidas de seguridad adecuadas puede exponer a la organización a vulnerabilidades significativas.

Además, la creciente cantidad de amenazas que sufren las organizaciones en los sistemas de información al interior y exterior hace que surja la necesidad de un diseño de una propuesta metodológica para la gestión de la seguridad de la información en la infraestructura tecnológica en el cabildo indígena resguardo de jambaló donde se minimicen dichas amenazas.

Mediante la Norma ISO 27001 que es un estándar internacionalmente reconocido para la seguridad de la información el cual ayuda en el fortalecimiento de los procesos para gestión de la

Seguridad de la Información en el Cabildo Indígena Resguardo de Jambaló y proporcionará una guía clara para la gestión de la seguridad de la información.

Con el desarrollo de la propuesta metodológica para la gestión de la seguridad de información contribuye al empoderamiento de los miembros que trabajan en el cabildo para tomar decisiones sobre el uso adecuado de los sistemas de información, el uso de la tecnología y la protección de sus datos personales, esto contribuye a la sostenibilidad del cabildo indígena resguardo de jambaló en un mundo más digitalizado.

1.3. OBJETIVOS

1.3.1. Objetivos General:

- Diseño de una Propuesta Metodológica para la Gestión de la Seguridad de la Información en la infraestructura tecnológica del Cabildo Indígena, Resguardo de Jambaló.

1.3.2. Objetivo Específicos:

- Analizar normativas, estándares y buenas prácticas internacionales en gestión de la seguridad de la información aplicables al contexto del Cabildo Indígena.
- Diagnosticar el estado actual de la infraestructura tecnológica y de la gestión de la seguridad de la información en el Cabildo Indígena del Resguardo de Jambaló.
- Identificar los activos informáticos de la organización para establecer los dominios de la norma ISO 27001
- Elaborar un plan de políticas y procedimientos claros y específicos para la Seguridad de la Información en el contexto del Cabildo Indígena, Resguardo de Jambaló.

1.4. MARCO TEÓRICO

La presente investigación del sistema de gestión de seguridad de la información en la infraestructura tecnológica en el cabildo indígena resguardo de Jambaló, tiene como objetivo utilizar conceptos referentes a la seguridad de la información esto conlleva que las organizaciones generen buenas prácticas seguridad y ventajas competitivas mejorando la efectividad, eficiencia y eficacia en la calidad de las políticas y procedimientos al aplicar a cualquier tipo de entidad.

1.4.1. *La seguridad de la información como pilar organizacional*

En la sociedad contemporánea, caracterizada por la digitalización de procesos y la interconexión global, la información se ha consolidado como uno de los activos más valiosos para organizaciones de todo tipo. Su importancia radica en que sustenta la toma de decisiones, la prestación de servicios y la construcción de confianza con los grupos de interés (Whitman & Mattord, 2022).

La seguridad de la información se entiende como la protección de la confidencialidad, integridad y disponibilidad de los datos frente a amenazas que puedan comprometer su almacenamiento, transmisión o uso (International Organization for Standardization [ISO], 2022). Estos principios garantizan que la **confidencialidad** impida accesos no autorizados, la **integridad** preserve la exactitud y consistencia de los datos, y la **disponibilidad** asegure el acceso oportuno a la información cuando sea requerido.

En ausencia de medidas de protección adecuadas, las organizaciones enfrentan riesgos como la pérdida de datos, el daño reputacional, la interrupción de servicios y el incumplimiento normativo (González & Ramírez, 2021). Estos riesgos resultan aún más relevantes en

instituciones comunitarias, en las que la información no solo respalda la gestión administrativa, sino que también se vincula a la memoria cultural y a la confianza social.

1.4.2. Sistema de Gestión de Seguridad de la Información

Moreno Vásquez, M., Guzmán Granada, J. (2011). Propuesta de implementación de un sistema de gestión de seguridad de la información integrado al sistema de gestión de calidad actual de la Universidad Tecnológica de Pereira. Colombia: Universidad Tecnológica de Pereira. Facultad de Ingenierías Eléctrica, Electrónica, Física y Ciencias de la Computación. Especialización en Redes de Datos. La seguridad de la información actúa como un elemento que permite evitar o mitigar los riesgos pertinentes a la información, tanto en el sector público como en el privado. Un Sistema de Gestión de Seguridad de la Información consiste como su nombre lo sugiere en la implementación de un conjunto apropiado de controles, incluyendo políticas, para la administración de la información.

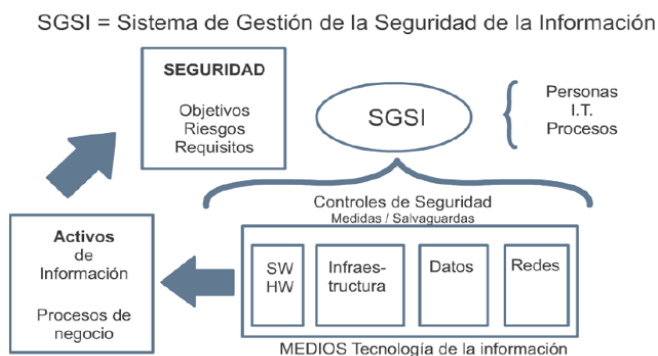


Figura 1 Sistema de gestión de seguridad

1.4.3. Norma ISO/IEC 27001 2022: y el Sistema de Gestión de Seguridad de la Información

Según Camargo, Erney Alberto Ramírez, & Pinzón, Miguel Alberto Rinconc. (2022) aborda la importancia que ha tomado la iso 27001 en entidades públicas en la protección de la informacion lo cual enfatiza la transparencia de los procesos eficientes en el nivel de cumplimiento en la seguridad digital.

La norma ISO/IEC 27001: establece los requisitos para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI). Este sistema proporciona un marco formal y estructurado para proteger los activos de información de cualquier organización (ISO, 2022).

El modelo se fundamenta en el ciclo de mejora continua PHVA (Planear, Hacer, Verificar y Actuar), lo que garantiza que los controles de seguridad evolucionen frente a nuevas amenazas. La norma contempla aspectos como el contexto organizacional, la definición de roles y responsabilidades, la gestión de riesgos, el soporte y desarrollo de competencias del personal, la implementación de controles, la auditoría de desempeño y la mejora continua.

En su actualización de 2022, la norma incorpora mayor énfasis en la ciberseguridad y la protección de datos personales, temas especialmente relevantes ante el incremento de ataques cibernéticos a nivel global (ISO, 2022).

1.4.4. Norma ISO 31000:2018 y la cultura de gestión del riesgo

La ISO 31000:2018 ofrece lineamientos universales para la gestión de riesgos en cualquier tipo de organización. Su objetivo es integrar la cultura de prevención y resiliencia en la planeación y operación de las instituciones (ISO, 2018).

Los principios que promueve son la integración, la adaptabilidad, la transparencia y la mejora continua. Esta norma resalta la necesidad de incluir a los actores involucrados en la toma de decisiones, lo cual facilita su aplicación en contextos comunitarios, donde el trabajo colaborativo constituye un valor fundamental (Ramírez & López, 2020).

1.4.5. Aplicación de las normas en contextos comunitarios

La implementación de marcos de seguridad en comunidades indígenas representa tanto retos como oportunidades. Entre los desafíos se encuentran la escasez de recursos económicos, el bajo acceso a capacitación especializada y la dependencia de infraestructuras externas, como los proveedores de internet. Sin embargo, la cultura comunitaria fortalece el proceso gracias a valores como la colectividad, la confianza y el compromiso social.

Diversos estudios en América Latina han mostrado que la aplicación conjunta de la ISO 27001 y la ISO 31000 no solo mitiga riesgos tecnológicos, sino que también fortalece la autonomía administrativa de las comunidades (Ramírez & López, 2020).

Según Castro Santana, Carmen Lizbet, León Robaina, Rosario, & Estrada Hernández, José Armando. (2024) plantea que las organizaciones actualmente están expuestas a numerosos riesgos dada a la variedad de actividades que desarrollan

En este sentido, el Cabildo Indígena Resguardo de Jambaló puede beneficiarse mediante:

- La definición de políticas de seguridad alineadas con estándares internacionales y su identidad cultural.
- La identificación de activos críticos (equipos tecnológicos, información administrativa, medios de comunicación comunitarios).
- El diseño de un plan de tratamiento de riesgos ajustado a su realidad social y tecnológica.
- La generación de conciencia comunitaria sobre el uso seguro de la tecnología.

1.4.6. Seguridad informática

Chicano Tejada Ester (2016), la seguridad informática es una disciplina que se ocupa de proteger la integridad, confidencialidad y disponibilidad de la información en sistemas informáticos. Es un campo amplio que abarca una variedad de tecnologías, procesos y prácticas diseñadas para proteger los sistemas, redes, programas y datos de ataques, daños o accesos no autorizados.

Aquí hay algunos conceptos clave en seguridad informática:

- **Confidencialidad:** Se refiere a la protección de la información sensible para prevenir su acceso no autorizado. Esto implica el uso de técnicas como la encriptación para proteger datos confidenciales.
- **Integridad:** Garantiza que la información no sea alterada de manera no autorizada. Se utilizan medidas como firmas digitales y para detectar cambios no deseados en los datos.

- **Disponibilidad:** Asegura que los sistemas y datos estén disponibles y accesibles cuando sea necesario. Esto implica la implementación de medidas para prevenir interrupciones y garantizar la continuidad del negocio.
- **Autenticación:** Verificación de la identidad de un usuario, dispositivo o sistema. Contraseñas, tarjetas inteligentes y biometría son métodos comunes de autenticación.
- **Autorización:** Determina qué acciones o recursos específicos están permitidos para usuarios autenticados. Se establecen políticas y permisos para controlar el acceso.
- **Firewalls:** Dispositivos que controlan el tráfico de red basándose en reglas predefinidas. Ayudan a prevenir accesos no autorizados y proteger redes contra amenazas.
- **Antivirus y Antimalware:** Software diseñado para detectar, prevenir y eliminar software malicioso, como virus, gusanos y troyanos.
- **Actualizaciones y Parches:** Mantener todos los sistemas actualizados con los últimos parches de seguridad es crucial para cerrar vulnerabilidades conocidas.
- **Educación y concienciación:** La formación del personal y la concienciación sobre prácticas de seguridad son aspectos fundamentales. Los usuarios informados son menos propensos a caer en trampas y ser víctimas de ataques.
- **Análisis de Vulnerabilidades y Pruebas de Penetración:** Identificar y corregir debilidades en sistemas y redes antes de que sean explotadas. Las pruebas de penetración simulan ataques para evaluar la resistencia de un sistema.

- **Cifrado:** La codificación de datos para que solo aquellos autorizados puedan acceder a la información. Se utiliza en comunicaciones, almacenamiento y otras áreas para proteger la confidencialidad.
- **Gestión de Incidentes:** Preparación y respuesta a incidentes de seguridad para minimizar el impacto y restaurar la normalidad lo más rápido posible.

La seguridad informática es un desafío constante debido a la evolución de las amenazas y tecnologías. La implementación de un enfoque integral y actualizado es esencial para proteger la información en entornos digitales cada vez más complejos.

1.4.7. Políticas de seguridad informática

El objetivo fundamental de las políticas de seguridad consiste en proporcionar orientación y las direcciones para la seguridad, de acuerdo con los requisitos de la organización y las leyes vigentes. Las políticas de seguridad son documentos que establecen las reglas, directrices y procedimientos que una organización debe seguir para proteger sus activos de información y garantizar un entorno seguro. Estas políticas forman parte integral de un programa de seguridad de la información y son esenciales para mantener la integridad, confidencialidad y disponibilidad de los datos, generalmente se abordan en las políticas de seguridad:

- **Política de contraseñas:** Establece los requisitos para la creación, uso y gestión de contraseñas seguras. Puede incluir pautas sobre la frecuencia de cambio de contraseñas y la prohibición de compartir contraseñas.

- **Política de Acceso:** Define quién tiene acceso a qué recursos y bajo qué condiciones. Puede abordar el principio de privilegios mínimos, que sostiene que los usuarios deben tener solo el acceso necesario para realizar sus funciones.
- **Política de Uso Aceptable:** Establece las reglas para el uso aceptable de los activos de información, incluyendo hardware, software y redes. Puede abordar temas como la prohibición de actividades no autorizadas, la descarga de software no aprobado y el acceso a sitios web no relacionados con el trabajo.
- **Política de Protección de Datos:** Define cómo se deben manejar, almacenar y transmitir los datos, especialmente los datos sensibles o personales. Puede abordar la encriptación de datos, la clasificación de datos y la notificación de brechas de seguridad.
- **Política de Copias de Seguridad:** Establece las prácticas para realizar copias de seguridad periódicas de datos críticos y la recuperación de la información en caso de pérdida o daño.
- **Política de Seguridad Física:** Define las medidas de seguridad física para proteger los activos de información, como restricciones de acceso a las instalaciones y protección contra desastres naturales.
- **Política de Seguridad de Red:** Establece las medidas de seguridad para proteger la red de la organización, incluyendo firewalls, detección de intrusiones y políticas de seguridad de Wifi.
- **Política de Dispositivos Móviles:** Aborda el uso seguro de dispositivos móviles propiedad de la organización o utilizados para acceder a los recursos de la empresa.

- **Política de Gestión de Incidentes:** Establece los procedimientos a seguir en caso de una violación de seguridad o incidente.
- **Política de Cumplimiento y Auditoría:** Define cómo se llevarán a cabo las auditorías internas y externas para garantizar el cumplimiento de las políticas y regulaciones de seguridad.

1.4.8. Controles de seguridad

Los controles de seguridad son medidas y acciones implementadas para proteger los activos de información y garantizar la seguridad de los sistemas y datos de una organización. Estos controles se pueden clasificar en varias categorías según su función y objetivo. Estos controles están diseñados para garantizar la confidencialidad, integridad y disponibilidad de la información.

Controles



Figura 2 Norma ISO 27001 POR ESTEBAN SAN ROMAN CYNTHUS

1.4.9. Modelo PHVA aplicado a los procesos SGSI

ISO 27001: La implementación de un Sistema de Gestión de Seguridad de la Información mediante el ciclo PHVA. sotools.us El modelo PDCA (Plan, Do, Check, Act), también conocido como el ciclo de mejora continua, es una metodología de gestión que se puede aplicar a diversos procesos, incluidos los relacionados con los Sistemas de Gestión de Seguridad de la Información (SGSI)

Planifica	Establecer políticas, los objetivos, procesos y procedimientos que sean necesarios para gestionar los riesgos y mejoras con el fin de entregar resultados acordes con las políticas de seguridad.
Hacer	garantizar los respectivos procedimientos adecuados de los controles seleccionados para su correcta aplicación.
Verificar	evaluar los factores aplicables y verificar el desempeño de los procesos contra las políticas y los objetivos de seguridad y reportar los resultados previos para su revisión.
Actuar	emprender acciones preventivas y correctivas basadas en los resultados de verificación y revisión para minimizar los riesgos y así lograr una mejora continua de sgsi.

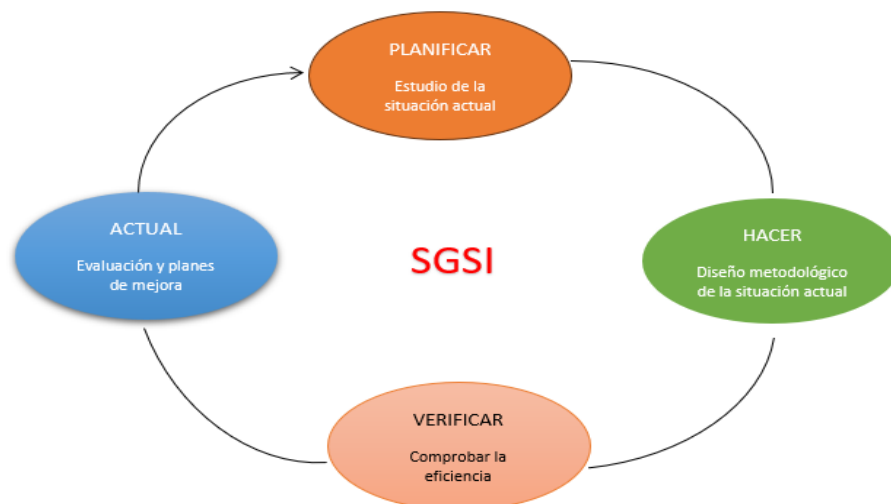


Figura 3 Ciclo PHVA en un SGSI

- **ESTUDIO DE LA SITUACIÓN ACTUAL:** En esta primera etapa del proyecto se presenta un análisis detallado para identificar las diferentes situaciones que afectan la seguridad en el cabildo indígena de jambaló
- **DISEÑO METODOLÓGICO:** En esta segunda etapa se diseñará una propuesta metodológica PMBOK, para la gestión de riesgos y se tomará como referencia la norma ISO 27001, para implementar los controles y políticas de seguridad pertinente
- **COMPROBACIÓN DE EFICIENCIA:** En esta tercera etapa se busca monitorear y revisar los errores generados de los resultados obtenidos, se debe detectar y prevenir.
- **EVALUACIÓN Y PLANES DE MEJORA:** Se establecerán acciones y recomendaciones de posibles planes de mejora

1.5. MARCO LEGAL:

Según Guzmán, P. K. *ISO 27001*. Es una norma desarrollada por ISO (organización internacional de Normalización) con el propósito de ayudar a gestionar la Seguridad de la Información en una empresa

La nomenclatura exacta de la Norma actual es ISO/IEC 27001 que es la revisión de la norma en su primera versión que fue publicada en el año 2005 como una adaptación de ISO de la norma británica BS 7799-2.

El certificado ISO 27001 le interesa a cualquier tipo de empresa sin importar su tamaño y actividad. El factor clave para decidir sobre la implantación de un sistema de gestión de la seguridad de la información radica en la importancia que los activos de información tienen dentro de una organización como elementos imprescindibles para la obtención de sus objetivos.

Según estadísticas de la Norma ISO, a nivel mundial la norma ISO 27001 es la norma de referencia para certificar la seguridad de la información en las organizaciones. De hecho, actualmente en España contamos con cerca de 800 empresas certificadas de un total de 33.000 certificados a nivel mundial.

(Decreto 1078 de 2015 Sector de Tecnologías de la Información y las Comunicaciones - Gestor Normativo, s. f.) este decreto tiene como propósito la privacidad y seguridad de la información lo cual reglamenta diferentes artículos que ayudan a mejorar la confidencialidad de la información además han sido utilizados por las diferentes organizaciones como del sector público o privado a nivel territorial.

1.6. Normativas, estándares y buenas prácticas internacionales en gestión de la seguridad de la información aplicables al contexto en el Cabildo Indígena resguardo de Jambaló.

Para el cabildo indígena resguardo de jambalo es importante adoptar normativas, estándares y buenas prácticas internacionales en gestión de seguridad de la información, considerando respetar su autonomía y tradiciones, al tiempo que protejan sus datos y sistemas. Se busca integrar la legislación colombiana sobre pueblos indígenas y las recomendaciones de organismos internacionales, además de estándares como ISO 27001 para la gestión de la seguridad de la información.

Normativas y estándares relevantes:

- **Constitución Política de Colombia:** Reconoce la diversidad étnica y cultural de la nación y establece la protección de los derechos de los pueblos indígenas, incluyendo sus territorios y autonomía.
- **Convenio 169 de la OIT:** Reconoce el derecho de los pueblos indígenas a la consulta previa, libre e informada sobre asuntos que les afecten, incluyendo la gestión de sus territorios y recursos.
- **Ley 21 de 1991:** Esta ley, que ratifica el Convenio 169 de la OIT, establece la obligación del Estado colombiano de garantizar la participación de los pueblos indígenas en la toma de decisiones que les afecten, incluyendo la gestión de sus datos.
- **Declaración de las Naciones Unidas sobre los Derechos de los Pueblos Indígenas:** Establece principios para el respeto y la protección de los derechos de los pueblos

indígenas, incluyendo su derecho a la autonomía, la autodeterminación y la gestión de sus recursos.

- **Decreto Ley 4633 de 2011:** Desarrolla los derechos de los pueblos indígenas en relación con su territorio, cultura, y formas de gobierno.
- **Decreto 2164 de 1995:** Reglamenta los resguardos indígenas, estableciendo su propiedad colectiva y sus características de inalienabilidad, imprescriptibilidad e inembargabilidad.
- **ISO 27001:** Estándar internacional para la gestión de la seguridad de la información, que proporciona un marco para proteger la confidencialidad, integridad y disponibilidad de la información.

CAPITULO 2

2. METODOLOGÍA

Para el desarrollo de la presente propuesta se ha tomado como referencia la Norma ISO 27001/31000 que está enfocado en las buenas prácticas de seguridad y análisis de riesgos, el proyecto está orientado de acuerdo a los objetivos específicos propuesto con el fin de alcanzar el objetivo general. Lo cual se pretende abordar varios procedimientos en los cuales se establecen los lineamientos de seguridad de la información en el cabildo indígena, con el fin de garantizar la aplicabilidad del sistema de gestión de seguridad.

Además, para el desarrollo del proyecto se utilizará el método de investigación de campo, que permite realizar un análisis sistemático de forma cuantitativo del problema de la organización, lo cual este método de investigación nos permite recolectar información, conocer su naturaleza y explicar sus causas y efectos a partir de datos o fuentes de forma directa, mediante encuestas, visitas de campo

2.1. INSTRUMENTOS PARA LA RECOLECCION DE INFORMACION

Para el presente desarrollo de la propuesta del proyecto de grado se utilizó el siguiente mecanismo para la recolección de información.

- Encuestas

2.2. FASES METODOLÓGICAS

Teniendo en cuenta en la norma ISO/IEC 27001, los requerimientos necesarios para establecer el diseño una propuesta metodológica para la implementación de un modelo para la gestión de la seguridad de la información en la infraestructura tecnológica en el cabildo indígena resguardo de Jambaló, se establecieron las siguientes fases para el desarrollo del proyecto.

Fase 1 Estudio diagnóstico de la situación actual: Teniendo en cuenta la metodología de investigación en esta fase corresponde a los pasos para identificar el manejo de seguridad de acuerdo al nivel de madurez que tiene la organización indígena.

A continuación, se presentan los mecanismos desarrollados en la investigación.

- Evidencias de campo
- Diligenciamiento de encuesta con el objetivo de mirar el nivel de manejo de seguridad.
- Documentación existente por la organización indígena.

Fase 2 Contexto organizacional: en esta fase se desarrollan las diferentes actividades de investigación del contexto organizacional del cabildo indígena para establecer la gestión de seguridad.

Fase 3 Planificación del sgsi: en esta fase se establece los mecanismos de identificación de activos de información, los diferentes riesgos seguridad y se establece las políticas de seguridad tomado como referencia la Norma ISO/IEC 27001

CAPÍTULO 3

3. DISEÑO UNA PROPUESTA METODOLÓGICA PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN LA INFRAESTRUCTURA TECNOLÓGICA EN EL CABILDO INDÍGENA RESGUARDO DE JAMBALÓ.

A continuación, corresponde al desarrollo de las actividades de los componentes que se definieron para el diseño una propuesta metodológica para la gestión de la seguridad de la información en la infraestructura tecnológica en el cabildo indígena resguardo de Jambaló, las cuales contemplan una serie de actividades que permiten alcanzar los objetivos propuestos.

Además, a lo largo de este documento se puede evidenciar los diferentes medios utilizados para la realización de la investigación del proyecto, así mismo se puede evidenciar las actividades desarrolladas en los estudios metodológicos especificados.

3.1. El alcance y límites del proyecto

Para el desarrollo del proyecto, se garantiza la identificación de los elementos para el diseño una propuesta metodológica para la gestión de la seguridad de la información en la infraestructura tecnológica en el cabildo indígena resguardo de Jambaló, lo cual abarca la primera etapa que es controlar la situación actual de la información e identificar los posibles riesgos de acuerdo al diagnóstico recolectado de los factores internos, pero queda a disposición de las autoridades indígenas para la ampliación del proyecto y establecer los parámetros necesarios para la aplicabilidad de acuerdo a la normatividad ISO 27001/ISO 31000, respetando las normas de usos y costumbres como organización indígenas.

3.2. Fase 1- Diagnostico del estado actual de la infraestructura tecnológica y de la gestión de la seguridad de la información en el Cabildo Indígena del Resguardo de Jambaló:

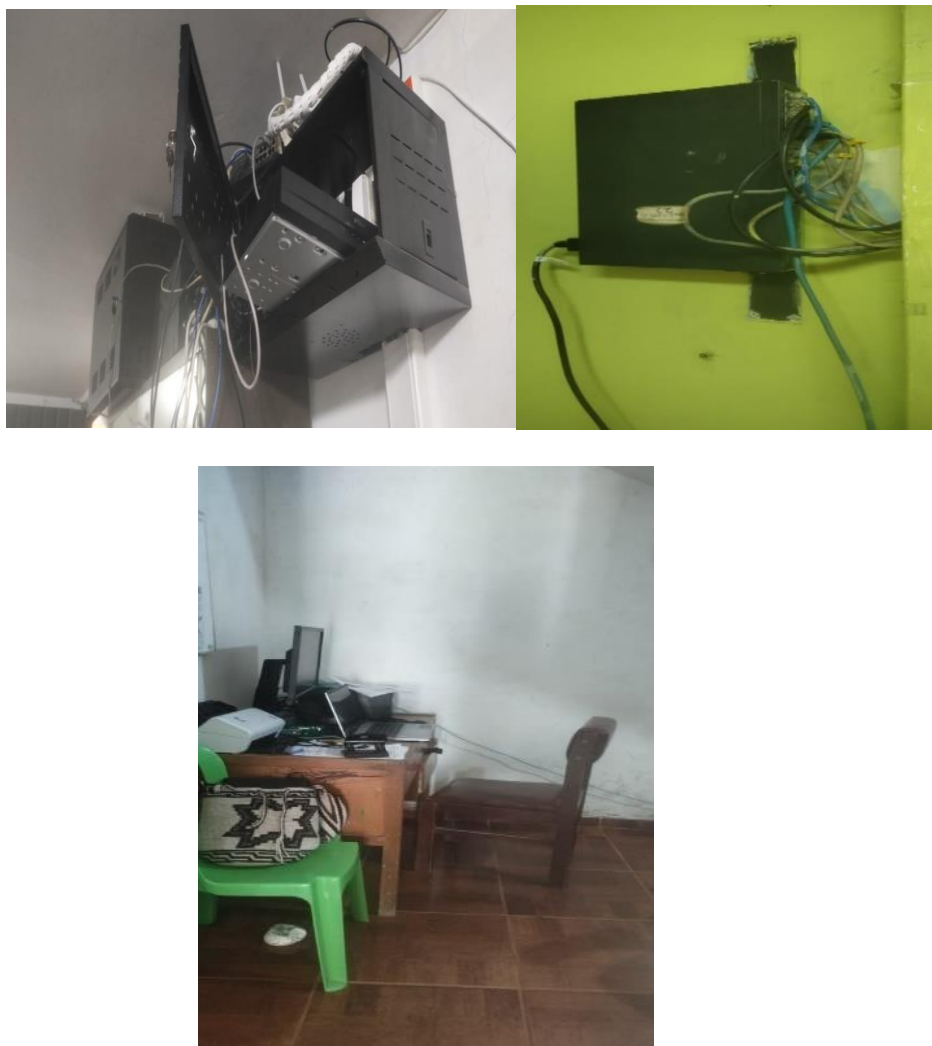
En esta primera etapa del proyecto se presenta un análisis detallado para identificar las diferentes situaciones de riesgos de seguridad que afectan en el cabildo indígena de jambaló lo cual se realizó el diagnóstico con el objetivo de conocer la situación inicial y así establecer el sistema de gestión de seguridad de la información, respetando la autonomía y el desarrollo del cabildo indígenas Jambaló.

Teniendo en cuenta el desarrollo proyecto se realizó una investigación de campo y de la normatividad de la iso 27001, además se realizó una encuesta al personal del cabildo que actualmente está laborando con el fin de conocer el impacto de manejo de seguridad así mismo se verifico varias visitas a las instalaciones del cabildo para conocer la situación y las condiciones de la organización actualmente.

3.2.1. Evidencia de campo

Para identificar la situación actual de la organización lo primero que se realizó fue visitas de campo en la cual se constató que el cabildo indígena no contaba con un manual de políticas de seguridad de la información de igual manera se tomaron evidencias de las malas prácticas del estado actual de los equipos de información.

A continuación, se presenta las evidencias de las malas prácticas del uso inadecuado de los aparatos tecnológicos.



3.2.2. Encuesta

Para el desarrollo del proyecto se utilizó un mecanismo fundamental para el análisis del impacto y conocer el estado teniendo en cuenta la línea de investigación. Para realizar la encuesta se encuestó a 20 empleados del cabildo indígena los cuales se puede evidenciar el nivel de falencias, la organización cuenta con 25 empleados que trabajan en las instalaciones del cabildo.

A continuación, se realizó una encuesta a 20 empleados del cabildo indígena de Jambaló donde se pudo constatar las malas prácticas de seguridad utilizadas en la organización.

¿Existen documentos de políticas y controles de seguridad en el Cabildo Indígena, Resguardo de Jambaló?

Mediante la realización de la encuesta al personal se pudo analizar que el 95% de los funcionarios encuestados respondieron que actualmente el cabildo no cuenta con políticas y controles de seguridad de la información lo cual pone en riesgo los activos de la organización.

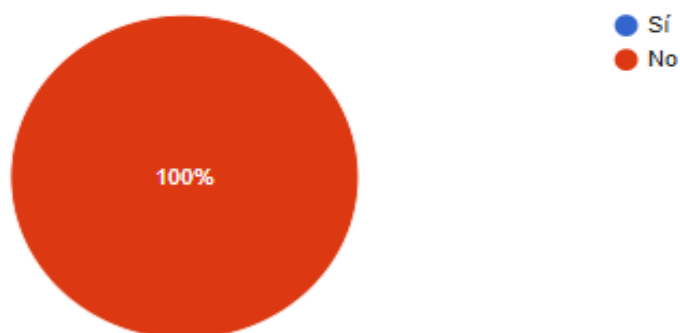


¿Usted como personal del cabildo indígena tiene conocimiento de los sistemas de gestión de seguridad?

Teniendo en cuenta la encuesta se pudo analizar que 100% del personal no tiene los conocimientos necesarios en la seguridad de la información lo cual es un riesgo para la organización además no cuentan con la capacitación necesaria del personal que labora así mismo tiene un alto grado de riesgo de pérdida de información ya que ya que no cuenta con medios para salvaguardar la información.

¿Usted como personal del cabildo indígena tiene conocimiento de los sistemas de gestión de seguridad ?

20 respuestas



¿Qué medios o estrategias utiliza para evitar acceso no autorizado, de informacion confidencial de la organización?

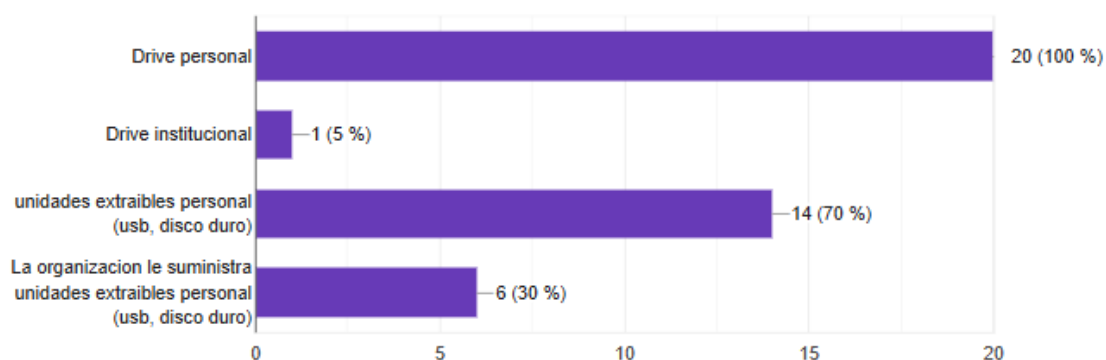
Se pudo constatar mediante la encuesta que el personal del cabildo indigena resguardo de Jambaló utiliza como medio de seguridad su drive personal para guardar informacion

confidencial de la organización lo cual el cabildo está expuesto a pérdidas o robo de información, de igual manera con un 70% de los encuestados utilizan unidades extraíbles personales para guardar la información lo que genera riesgos por pérdida.

¿Que medios o estrategias utiliza para evitar acceso no autorizado de información confidencial de la organización?)

 Copiar gráfico

20 respuestas



Teniendo en cuenta el desarrollo de la investigación con la realización de la encuesta y además las visitas de campo al cabildo indígena de Jambaló se pudo identificar las siguientes situaciones que están afectando la organización.

- No se evidencia políticas de seguridad
- Falta de un comité de seguridad de la información
- No se evidencia controles de seguridad
- No se tiene inventario de todos los activos
- No hay responsabilidad de las personas que laboran en la organización
- No cuentan con restricciones de los aparatos tecnológicos como celulares o computadores externos
- Falta de jornadas de capacitación de los funcionarios en seguridad de la información

- No hay restricciones de unidades extraíbles de la información de la organización
- Presentan déficits de seguridad de la información
- No cuenta con medios de seguridad física

3.3. Fase 2 – Contexto organizacional

En esta fase del proyecto tiene como propósito conocer la estructura de la organización en el contexto administrativo teniendo en cuenta la norma ISO/IEC 27001 así establecer los factores interno y externos y estar alineados al cumplimiento normativo de seguridad

3.3.1. Naturaleza del cabildo indígena resguardo Jambaló.

El Cabildo Indígena Resguardo de Jambaló Cauca, entidad pública de carácter especial, sin ánimo de lucro, legalmente constituida por el ministerio del interior tiene una estructura política organizativa administrable de acuerdo a la ley de origen y derecho mayor, así como las normas contempladas en la ley 89 de 1980, los artículos 93, 246, 330 de la constitución política de Colombia, la declaración de las Naciones Unidas sobre los derechos de los pueblos indígenas y el convenio 169 de la OIT aprobada mediante la ley 21 de 1991.

En la constitución del 1991 ratifica los derechos de las organizaciones indígenas en la cual el decreto 1953 de 2014 garantiza la autonomía para administrar los recursos propios como régimen especial con el fin de poner en funcionamiento los territorios indígenas respecto de la administración de los sistemas propios de los pueblos indígenas hasta que el congreso expida la ley de qué trata el artículo 329 de la Constitución Política.

El Cabildo Indígena Resguardo de Jambaló tiene una estructura política administrativa que a lo largo del tiempo ha permitido avanzar en los proyectos comunitarios orientados desde las asambleas con el propósito de avanzar en el desarrollo educativo, económico, salud y gobierno propio.

El cabildo indígena resguardo de Jambaló, es una empresa comunitaria. Está ubicado al nororiente del departamento del Cauca, a 80 kilómetros de la ciudad de Popayán. Limita por el norte con los municipios de Caloto y Toribío, por el oriente con el municipio de Páez, por el sur con el municipio de Silvia y por el occidente con los municipios de Caldono y Santander de Quilichao, en (Radioteca.net.) el cabildo indígena está conformado por las Autoridades Tradicionales Nej Kwe'sx quienes por el mandato propio elegidos por la comunidad en la asamblea son las garantes y orientadores del cumplimiento de los derechos en defensa del territorio y de la autonomía política, jurídica o normativa, financiera y económica; fiscal, administrativa, cultural; de sus tradiciones espirituales, de su historia y de su ciencia como pueblos indígenas.

se plantea realizar una propuesta metodológica para la implementación de un modelo para la gestión de la seguridad de la información en la infraestructura tecnológica en el cabildo indígena resguardo de Jambaló con el fin de salvaguardar los activos informáticos que tiene el cabildo indígena y prevenir de riesgo de pérdida información que se genera.

3.3.2. Surgimiento del plan de vida proyecto global

(¿QUIENES SOMOS? (s/f). Proyecto Global Jambaló.org.). El Proyecto Global nace el 22 de diciembre de 1986 en una reunión que se realizó en la cabecera municipal de Jambaló, encabezada por el gobernador del cabildo Isidro Dagua, José María Dagua, Francisco Gembuel, cabildantes de las veredas y el padre Mauro Riascos, entre otros, teniendo como ejemplo El PROYECTO NASA fundado por el padre Álvaro Ulcué Chocue en Toribío.

En esta reunión se analizó la situación social y económica de la comunidad tratando de dar alternativas para su desarrollo, por tal motivo se programó una asamblea en La Mina para el 3 de marzo de 1987, donde se decidió implementar un proyecto de vida propio bautizándose con el nombre: **PROYECTO GLOBAL**. El objetivo principal era evaluar la situación actual del resguardo y municipio en cuanto a lo organizativo y fortalecer la autoridad del cabildo buscando el desarrollo integral de la comunidad en lo político, económico, social y cultural. Se tuvieron en cuenta otros objetivos:

- Mirar las dificultades que se presenten en cada vereda
- Plantear soluciones en forma colectiva
- Evaluar las diferentes organizaciones
- Interactuar en el Resguardo y Municipio de Jambaló.

Desde ese entonces, la Asamblea del Proyecto Global se realiza cada tres meses, presidida generalmente de una reunión de todos sus programas para organizar el plan de trabajo con el fin de evaluar los diferentes procesos de desarrollo y plantear las alternativas de solución a las dificultades en conjunto con la comunidad. Participan las treinta y seis veredas y actualmente,

los cuatro barrios del casco urbano. La asamblea se realiza con el aporte económico y humano de las comunidades.

La asamblea del Proyecto Global es también la plataforma sobre la que se sustenta el proyecto político de las comunidades. Es un espacio de decisión, de participación y de capacitación. El Movimiento Cívico les ha dado otra dimensión a las asambleas pues en ellas se hace la elección y concertación de los candidatos que representarán a la comunidad en las diferentes corporaciones a nivel del Municipio – Resguardo, Departamento y Nación.

- **VISIÓN:** Lograr de manera permanente una comunidad unida, organizada, solidaria, proyectada consciente educada y respetuosa, con cultura propia, con identidad, fortaleciendo los procesos y principios del Plan de Vida del movimiento indígena.
- **MISIÓN:** Mantenernos unidos en comunidad para continuar orientándola, organizándose y visualizando el proyecto de vida del Pueblo Nasa y misak en otros espacios y niveles organizativos desde lo Local, Zonal, Regional y Nacional.

3.3.3. ESTRUCTURA ORGANIZACIONAL

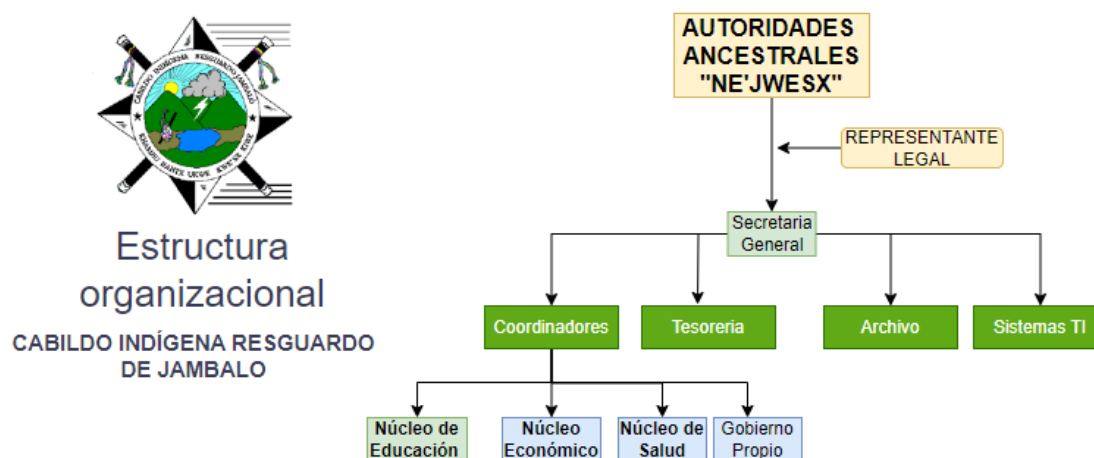


Figura 4 Estructura organizacional

3.3.4. Responsabilidad de las autoridades ancestrales

Los Nej Wesx “autoridades ancestrales” del resguardo indígena de jambalo - cauca, en uso de las facultades legales que le confiere la ley 89 de 1890, la constitución política de colombia en sus artículos 246 y 330 ratificados en el convenio 169 de la OIT ratificado en la ley 21 del 91 y desde la ley de origen y los mandatos comunitarios, lo cual las autoridades ancestrales en su función de autoridad establecida por la comunidad y de los apoyos técnicos es hacer que funcione el sistema de gestión de seguridad de la información.

se requiere que todas las decisiones tengan una trazabilidad con el buen manejo de las políticas de seguridad comprometiéndose con la implementación monitorización, revisión y

mejoras además el compromiso de las autoridades ancestrales y representante legal con el diseño de la propuesta metodológica para la implementación de un modelo para la gestión de la seguridad de la información en la infraestructura tecnológica en el cabildo indígena resguardo de Jambaló, muestra el compromiso como organización indígena para el desarrollo y el fortalecimiento de las buenas prácticas de las políticas de seguridad.

Compromisos:

- **Aprobar las Políticas de Seguridad de la Información.**
- **Definir los lineamientos para el contacto con las autoridades en caso que se requiera alguna intervención por parte de los mismos.**
- **Garantizar el funcionamiento de las políticas de seguridad:** Actualmente el cabildo indígena no cuenta con un sistema de seguridad de la información lo cual con la realización de las políticas y controles de seguridad se pueda direccionar el funcionamiento y garantizar la seguridad de los activos.
- **Aprobar los roles y responsabilidades de los funcionarios relacionados con la seguridad de la información:** Las autoridades ancestrales junto con la representante legal han direccionado el funcionamiento del cabildo lo cual se han creado los roles de apoyos técnicos, apoyo jurídico etc.
- **Asignar recursos, infraestructura física y personal necesario para la gestión de la seguridad de la información en la Organización:** En la asignación de los recursos es necesario la aprobación en las asambleas del proyecto global asignar los recursos necesarios para gestionar e implementar el proyecto en cada fase.
- **Llevar periódicamente cada 6 meses la intervención para garantizar y revisar el funcionamiento:** Las autoridades ancestrales junto a la representante

legal deben de revisar con el encargado de sistemas el funcionamiento de las políticas y controles de seguridad para garantizar el cumplimiento de las normas.

3.3.5. Comité Técnico de seguridad de la información.

Dentro el cabildo indígena se pudo establecer el comité técnico de seguridad de la información con el fin direccionar y buscar nuevas alternativas de seguridad para brindar apoyo al personal garantizando el funcionamiento de las normas establecidas.

Para garantizar el funcionamiento de las normas establecidas y velar por la seguridad de la información se establece un comité técnico de seguridad de la información en la infraestructura tecnológica del cabildo indígena resguardo de Jambaló que ayude a mitigar la seguridad de los activos y la información de la organización, además con la conformación de este apoyo técnico tiene como objetivo buscar un equilibrio y asegurar una dirección y en supervisión de las autoridades ancestrales, así mismo fomentar al personal que labore iniciativas propias sobre seguridad de la información, a través de un compromiso mutuo y el uso adecuado de los activos de la organización.

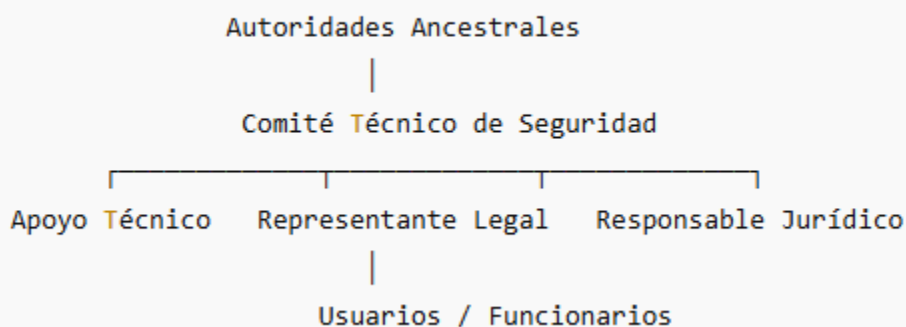
compromiso

- Propender por el cumplimiento de las políticas y las buenas prácticas de seguridad de la información consignadas en el manual.
- Generar nuevas políticas y actualizar las políticas de seguridad de la información consignadas en el manual.

- Realizar el monitoreo constante de los incidentes de seguridad detectados o reportados por otras dependencias y realizar la gestión correspondiente para mitigar o trasladar el mismo.
- Identificar y ejecutar controles para los riesgos identificados.
- Programar y ejecutar auditorías internas al Sistema de Gestión de Seguridad de la Información, con el fin de verificar si las políticas.

El comité de seguridad de la información está conformado de la siguiente manera:

- **Apoyo técnico de la seguridad de la información:** El apoyo técnico de seguridad es el encargado de administrar los dispositivos electrónicos como son los equipos de cómputo, revisar el funcionamiento preventivo, instalación de las herramientas informáticas.
- **Representante legal:** La representante legal se encarga de gestionar los recursos necesarios y velar por el cumplimiento de las normas como son las políticas de seguridad.
- **Autoridades ancestrales:** Las autoridades ancestrales son las encargadas de direccionar todo el funcionamiento de la organización del cabildo indígena y hacer cumplir junto a la representante legal del cabildo las políticas de seguridad y los controles de seguridad.
- **Responsable jurídico:** El personal jurídico es el encargado de vigilar el cumplimiento y sancionar de acuerdo con la decisión tomada por las autoridades ancestrales.



3.4. Fase 3 Planificación del SGSI

En esta fase del proyecto se llevaron a cabo diferentes actividades de clasificación de activos, para desarrollar la propuesta metodológica con el fin mitigar el alto nivel de criticidad de los activos para ello se establecieron los siguientes parámetros:

- **Tipos de activos:** se identifica los tipos de activos que tiene la organización
- **Identificación de activos:** la identificación de los activos es esencial en el proceso de desarrollo lo cual sirve como insumo para la identificación de riesgos
- **Clasificación y valoración de riesgo:** este es un proceso importante lo cual nos permite clarificar los activos de acuerdo a los principios de seguridad de la información como son la confidencialidad, integridad y disponibilidad
- **Confidencialidad:** para efectos de seguridad del presente proyecto no se estableció nombre de las bases de datos de la organización con el fin de proteger la información del cabildo indígena

3.4.1. Tipos de activos

En esta primera actividad en el proceso de recolección de información se identificaron los tipos de activos de la infraestructura tecnológica en el cabildo indígena resguardo de jambaló a continuación se estableció los siguientes tipos de activos Tabla 1.

Tipo de activos	
Tipo de activo	Descripción
Software	Programas informaticos, software, base de datos, sistema de información que el cabildo geranera o utiliza por parte de los colaboradores
Personal	Personas relacionadas con los sistemas de información
Equipos informáticos	Hardware. Medios materiales, fisicos, destinados a soportar directa o indirectamente los servicios que presta la organización
Soportes de información	Dispositivos fisicos que permiten almacenar información de forma permanente que el cabildo maneja
información	datos de gestión interna que los funcionarios manejan en la organización
sistemas de comunicación	informacion y equipos de comunicación que tiene la organizion

Tabla 1 Tipos de Activos

3.4.2. Identificación de los activos

Luego de identificar los tipos de activos se realizó el respectivo inventario de todos los activos que tiene el cabildo de Jambaló lo cual el estado de los activos es crítico ya que no cuenta con la seguridad pertinente.

a continuación, se realizó el siguiente inventario del cabildo de Jambaló Ver

(ANEXO 1).

inventario de activos de la informacion en el cabildo indigena de jambalo			
Nombre de activo	Descripcion de activo	Tipo de activo	Contenedor
Red wifi	los equipo de la organizacion indigena	Infraestructura del cabildo	Red LAN
Computadores	Computadores asignados a los colaboradores del cabildo	Equipos de computo	Computadores
Portatiles	Portatiles asignados a los colaboradores del cabildo	Equipos de computo	Portatiles
Camara de seguridad	Camaras de seguridad que se encuentran dentro de la organizacion	Equipos de seguridad	Camara de seguridad
Dispositivos de red	Dispositivos activos en el cabildo (switch,router)	Equipos de computo	switch,router
Pagina web	Pagina web del cabildo	Software	Servidores de aplicación
intranet	Pagina web del cabildo	Software	Servidores de aplicación
Bases de dato	bases de datos que utiliza el cabildo	Servicios	Bases de datos
sistemas de comunicación	sistema radial utilizado en la organizacion	Equipo de computo	sistema radial de comunicaciones
Antivirus	sistema de proteccion de de equipos de computo	Software	Servidores de aplicación

Tabla 2 Identificación de activos



Esta tabla es un diagnóstico del inventario de activos en la Infraestructura Tecnológica en el Cabildo Indígena, Resguardo de Jambaló, para llevar un control básico de los activos gestionados, así como de sus responsables, ubicación, y otras características relevantes.

La descripción de los campos es la siguiente:

- * **Cantidad:** cantidad del activo. que estan en cada oficina
- * **Responsable:** Nombre del responsable del activo. Se puede tratar de una persona concreta o de un departamento.
- * **Tipo:** El campo tipo se utiliza para clasificar los activos. Resulta conveniente distinguir si el activo es físico o si es lógico (intangible).
- * **Ubicación:** Indica dónde está ubicado físicamente el activo.
- * **Crítico:** Campo que indica si el activo juega un papel fundamental / imprescindible (crítico) para la organización.

INVENTARIO DE ACTIVOS				
cantidad	Tipo	Responsable	Ubicación	Crítico
1	computador mesa (físico)	Cordinador Nucleo de salud	oficina nucleo de salud	Sí
1	Switch	Cordinador Nucleo de salud	oficina nucleo de salud	Sí
1	computador mesa (físico)	Secretaria	oficina secretaria general	Sí
1	Impresora	Secretaria	oficina secretaria general	Sí
1	computador mesa (físico)	Encargado del Archivo	oficina de archivo	Sí
1	Impresora	Encargado del Archivo	oficina de archivo	Sí
7	computador mesa (físico)	Tesoreria	oficina de tesoreria	Sí
1	Impresora	Tesoreria	oficina de tesoreria	Sí
1	Switch	Tesoreria	oficina de tesoreria	Sí
1	Camara de seguridad	Tesoreria	oficina de tesoreria	Sí
2	computador mesa (físico)	comision Juridica	oficina comusion juridica	Sí
1	Switch	comision Juridica	oficina comusion juridica	Sí
1	Impresora	comision Juridica	oficina comusion juridica	Sí
3	computador mesa (físico)	Cordinado Nucleo Economico	oficina nucleo economico	Sí
1	Impresora	Cordinado Nucleo Economico	oficina nucleo economico	Sí
1	Switch	Cordinado Nucleo Economico	oficina nucleo economico	Sí
1	computador mesa (físico)	Guardia	oficina de la guardia	Sí
9	Camara de seguridad	Guardia	oficina de la guardia	Sí
2	computador mesa (físico)	P GLOB	oficina P GLOB	Sí
1	Impresora	P GLOB	oficina P GLOB	Sí
1	computador mesa (físico)	Autoridades ancestrales	oficina Autoridades ancestrales	Sí
1	Impresora	Autoridades ancestrales	oficina Autoridades ancestrales	Sí
5	Portatiles	Autoridades ancestrales	oficina Autoridades ancestrales	Sí
1	computador mesa (físico)	Representante Legal	oficina representante legal	Sí
1	Impresora	Representante Legal	oficina representante legal	Sí
5	computador mesa (físico)	cordinador semillas de vida	oficina semillas de vida	Sí
1	Router	cordinador semillas de vida	oficina semillas de vida	Sí
1	Impresora	cordinador semillas de vida	oficina semillas de vida	Sí
7	computador mesa (físico)	Cordinado Nucleo Educacion	oficina nucleo de educacion	Sí
1	Impresora	Cordinado Nucleo Educacion	oficina nucleo de educacion	Sí
1	Router	Cordinado Nucleo Educacion	oficina nucleo de educacion	Sí
2	computador mesa (físico)	Lenguas	oficina de Lenguas	Sí
1	Impresora	Lenguas	oficina de Lenguas	Sí
2	computador mesa (físico)	Mais planeacion-fondo	oficina Mais	No
1	Router	Auditorio	Auditorio	No
7	computador mesa (físico)	Cordinador de comunicaci3n	oficina emisora	No
1	computador mesa (físico)	PEC	oficina PEC	No
1	Impresora	PEC	oficina PEC	No

Tabla 3 activos

3.4.3. Criterios de fundamentales para la clasificación de activos

Para la clasificación de los activos en la organización primero se analizó los factores internos y externos que afecta el desarrollo de las actividades lo cual en la seguridad de la información es importante establecer directrices del manejo de la confidencialidad, disponibilidad e integridad en la seguridad de la información.

- **Confidencialidad:** Es importante tener en cuenta que la información suministrada en el cabildo indígena no estén disponibles ni revelada a individuos no autorizados lo cual el objetivo es prevenir y garantizar que la información interna y externa está protegida.
- **Integridad:** Hace referencia a la información que los funcionarios manejan dentro la organización que debe ser inalterada precisa que cuando se requiera la información está intacta sin alteraciones o modificaciones de acuerdo a las medidas de protección por establecer.
- **Disponibilidad:** Toda información que la organización genera debe estar disponible lo cual la no disponibilidad puede conllevar a un impacto y riesgo negativo alto por ende puede tener acciones legales a la organización como pérdida de información y sobre costos financieros.

3.4.4. Nivel de criticidad de los activos de la organización

Para identificar el nivel de criticidad de los activos se definió los siguientes pasos lo cual permite conocer el rango de cada uno.

A continuación, se realiza la siguiente tabla:

Nivel de criticidad de los activos del cabildo de jambalo		
Criterios de Evaluacion	valor Asignado	Nivel Criticidad
alto grado de criticidad que compromete la integridad, confidencialidad y disponibilidad del cabildo indigena	≥ 4	Alto
nivel medio de criticidad que compromete la integridad, confidencialidad y disponibilidad del cabildo indigena	$>2 \text{ a } < 4$	Medio
Nivel bajo de criticidad que compromete la integridad, confidencialidad y disponibilidad del cabildo indigena	$> 0 \text{ a } < 2$	Bajo
no compromete la integridad, confidencialidad y disponibilidad del cabildo indigena	igual a cero	No aplica

Tabla 4 Nivel de criticidad de activos

Por último se determinó el nivel de criticidad de los activos en el cabildo indigena de jambaló donde se analizó tres factores fundamentales para el desarrollo de la investigación que son la confidencialidad de los datos, la disponibilidad y la integridad lo cual en el cabildo el estado de criticidad es considerablemente vulnerables por la falta de un buen manejo y conocimiento de seguridad de la información ya que desde la misma autoridades ancestrales, la

representante legal y los apoyos técnicos no hay documentación sobre la seguridad de los activos y los sistemas de información.

Nivel de criticidad de los activos de los activos del cabildo indígena							
Nombre de activo	Descripción de activo	Tipo de activo	Contenedor	Valor de criticidad de activos			Nivel de criticidad
				Disponibilidad	Confidencialidad	Integridad	
Red wifi	Red wifi utilizado por los equipo de la organizacion indígena	Infraestructura del cabildo	Red LAN	4	5	4	Alto
Computadores	Computadores asignados a los colaboradores del cabildo	Equipos de computo	Computadores	4	4	5	Alto
Portatiles	Portatiles asignados a los colaboradores del	Equipos de computo	Portatiles	5	4	4	Alto
Camara de seguridad	Camaras de seguridad que se encuentran dentro de la organizacion	Equipos de seguridad	Camara de seguridad	3	3	3	Medio
Dispositivos de red	Dispositivos activos en el cabildo	Equipos de computo	switch,router	4	4	4	Alto
Pagina web	Pagina web del cabildo	Software	Servidores de aplicación	3	3	3	Medio
intranet	Pagina web del cabildo	Software	Servidores de aplicación	5	5	5	Alto
Bases de datos	bases de datos que utiliza el	Servicios	Bases de datos	5	5	4	Alto
sistemas de comunicación	sistema radial utilizado en la organizacion	Equipo de computo	sistema radial de comunicaciones	2	2	3	Medio
Antivirus	sistema de proteccion de de equipos de	Software	Servidores de aplicación	4	4	4	Alto

Tabla 5 Valoración de criticidad de activos

3.4.5. Valoración de Riesgos de seguridad

Mediante clasificación e identificación de activos y su respectiva la valoración del alto nivel de criticidad que se encuentra los activos en el Cabildo Indígena Resguardo de Jambaló. Se elaboró una Matriz de Análisis de Riesgos lo cual es un paso crucial para identificar, evaluar y gestionar los riesgos asociados con la seguridad de la información.

A continuación, se estableció los siguientes pasos para análisis de riesgos de seguridad:

- Identificación de riesgos
- Identificación de amenazas
- Identificación de vulnerabilidades
- Análisis y evaluación de impacto
- Cálculo de riesgo
- Medidas de mitigación

3.4.5.1. Identificación de riesgos de seguridad

Para la identificación de riesgos de seguridad de los activos y de la información que maneja el cabildo indígena de Jambaló se toma como referencia la norma ISO/31000 adaptando a la situación de la infraestructura actual de la organización.

Luego de verificar el estado de la situación de la organización en las visitas de las distintas oficinas que maneja el cabildo y de realizar las entrevistas a las personas que laboran se observó de los distintos procesos que llevan de acuerdo a su función o rol que desempeñan de la misma, con el objetivo de validar y determinar la situación actual de la seguridad de la información de todos los activos tecnológicos e información relacionado en el ANEXO 1 inventarios de activos se detectaron de las posibles amenazas que afectan la seguridad la de información del cabildo indígena, al igual de los controles pertinentes ANEXO A de la normatividad de la ISO 27001:2013. A continuación, se identifican unos hallazgos en las visitas realizadas al cabildo indígena resguardo de jambalo.

- No se evidencia políticas de seguridad
- Falta de un comité de seguridad de la información
- No se evidencia controles de seguridad

- No se tiene inventario de todos los activos
- No hay responsabilidad de las personas que laboran en la organización
- No cuentan con restricciones de los aparatos tecnológicos como celulares o computadores externos
- No hay restricciones de unidades extraíbles de la información de la organización
- No cuenta con medios de seguridad física

3.4.5.3. Identificación de Amenazas

Se identificaron las amenazas que puede afectar los activos de la organización de forma internas como externas a continuación se presenta una lista de riesgos que afecta la organización.

AMENAZAS QUE PUEDEN AFECTAR LOS ACTIVOS	
AMENAZAS	ACTIVOS
desastres naturales	instalacion inadecuada fluido electrico daños por incendios equipo de
Acceso no autorizado	administracion de informacion en los bases de datos
instalacion de software no autorizado	computadores, portatiles
modificacion sin autorizacion	bases de datos
perdida de equipos	area administrativas
perdida de informacion	directorios de activos bases de datos
estructuracion del cableado red	red LAN
abuso de privilegios	directorios de activos bases de datos

Tabla 6 Identificación de amenazas

3.4.5.4. Identificación de Vulnerabilidades:

Se identificaron las diferentes vulnerabilidades asociadas a las amenazas son debilidades que pueden ser explotadas:

VULNERABILIDAD ASOCIADO A LAS AMENAZAS		
AMENAZAS	ACTIVOS	VULNERABILIDAD
desastres naturales	instalacion inadecuada fluido electrico	ausencia de un sistema continuo
	daños por incendios equipo de computo	no hay exixtencia de seguridad
Acceso no autorizado	administracion de informacion en los equipos de	contraseñas no seguras
	bases de datos	inadecuada administracion de seguridad
instalacion de software no autorizado	computadores, portatiles	inadecuada administracion o asignacio de roles
modificacion sin autorizacion	bases de datos	inadecuada administracion
perdida de equipos	area administrativas	ausencia de vigilancia e inadecuado inventario de equipos
perdida de informacion	directorios de activos	inadecuada administracion
	bases de datos	error humano
estructuracion del cableado red	red LAN	Ausencia o inadecuado procedimiento de control de cambios
abuso de privilegios	directorios de activos	contraseñas no seguras
	bases de datos	inadecuada administracion

Tabla 7 Identificación de vulnerabilidades

3.4.5.5. Análisis y evaluación del Impacto riesgo:

Por medio del análisis de riesgo se estableció la evaluación del impacto potencial de cada amenaza sobre los activos identificados para establecer la probabilidad de ocurrencia mediante el impacto cuantitativo y cualitativo.

A continuación, se establece el impacto de riesgo de seguridad:

Análisis y evaluación del Impacto riesgo		
impacto	impacto cuantitativo	impacto cuantitativo
bajo	Pérdida mínima de datos o funciones, recuperable con poco esfuerzo en la organización.	no afecta la imagen de la organización y genera reprocesos menores que se puede recuperar
moderado	Pérdidas moderadas de datos o funciones, recuperable con esfuerzo considerable	afecta el desarrollo moderado de la seguridad se puede recuperar la información de la organización pero de poca calidad
alto	Pérdida crítica de datos o funciones, difícil o imposible de recuperar.	afecta la imagen de la organización no se puede recuperar financieramente y afecta la seguridad de la información

Tabla 8 Analisis y evaluación de riesgo

3.4.5.6. Evaluación de la Probabilidad

En la evaluar de la probabilidad de ocurrencia en la organización de acuerdo a los riesgos establecidos

• Probabilidad Baja: Rara vez ocurre.
• Probabilidad Moderada: Ocurre ocasionalmente
• Probabilidad Alta: Ocurre con frecuencia.

Tabla 9 Probabilidad de riesgo

3.4.5.7. Cálculo del Riesgo

De acuerdo al análisis de riesgo se estableció el proceso de amenaza asociados a los activos de la información combinado la probabilidad y el impacto de cada amenaza.

A continuación, se presenta la valoración de riesgo de los activos de la información

Valoracion de Riesgo					
AMENAZAS	ACTIVOS	Valor de impacto	Probabilidad	Riesgo	Medidas de mitigacion de riesgo
desastres naturales	instalacion inadecuada fluido electrico	Moderado	Alto	Alto	Respaldo de informacion copias de seguridad
	daños por incendios equipo de computo				
Acceso no autorizado	administracion de informacion en los equipos de	Alto	Moderado	Alto	planes de control control de usuarios
	bases de datos				
instalacion de software no autorizado	computadores, portatiles	Alto	Alto	Alto	capacitaciones
modificacion sin autorizacion	bases de datos	Alto	Alto	Alto	Respaldo de informacion
perdida de equipos	area administrativas	Moderado	Moderado	Moderado	control de seguridad
perdida de informacion	directorios de activos	Alto	Alto	Alto	copias de seguridad
	bases de datos				
estructuracion del cableado red	red LAN	Alto	Moderado	Moderado	adecuacion de cableado
abuso de privilegios	directorios de activos	Moderado	Moderado	Moderado	control de usuarios
	bases de datos				
Error humano	informacion	Alto	Alto	Alto	capacitaciones
Malware	equipo de computo	Alto	Alto	Alto	antivirus, actualizaciones
Falla en el Hardware	equipo de computo	Moderado	Bajo	Moderado	mantenimientos preventivos

Tabla 10 Calculo de riesgo

3.4.5.8. Medidas de Mitigación

A continuación, se realiza algunas recomendaciones a las autoridades ancestrales para mitigar cada riesgo identificado,

- ✓ **Capacitación y Concienciación:** Formar al personal sobre seguridad de la información.
- ✓ **Controles Técnicos:** Implementar firewalls, antivirus, y sistemas de detección de intrusos.

- ✓ **Políticas y Procedimientos:** Establecer y mantener políticas de seguridad claras.
- ✓ **Redundancia y Respaldo:** Asegurar la redundancia de sistemas críticos y realizar respaldos regulares.
- ✓ **Seguridad Física:** Mejorar la seguridad de las instalaciones físicas.

3.5. **POLÍTICAS DE SEGURIDAD**

A continuación, se desarrolló el manual de las políticas de seguridad para la infraestructura tecnológica del cabildo indígena resguardo de Jambaló, con el fin de mitigar los riesgos de seguridad, se tomó como referencia los lineamientos que brinda la norma ISO/IEC 27001, el ANEXO A Dominios objetivos de control.



Tabla 11 Norma ISO 27001

Objetivo

Establecer las políticas de seguridad de la información para el cabildo indígena resguardo de Jambaló, que se deben conocer y cumplir por todo el personal que labore en la organización sin importar el cargo de igual manera a terceros naturales o jurídicos que presten sus servicios o tenga alguna relación, con el fin de propender por la salvaguarda y preservación de la información, así como de los bienes y activos informáticos de la organización, garantizando la confidencialidad, integridad y disponibilidad de los mismos.

Alcance

Las políticas de Seguridad de la Información relacionadas en este manual, serán permeadas a todos los procesos estratégicos, de evaluación, misionales y de apoyo, estos lineamientos deberán ser socializados y cumplidos a cabalidad por todos los empleados administrativos, proveedores, contratistas y terceros, que tengan acceso a los sistemas de información e instalaciones físicas del cabildo indígena resguardo de jambaló.

Lineamiento de la política de seguridad

Toda información que se utilice en los equipos de cómputo en la infraestructura tecnológica del cabildo indígena resguardo de Jambaló será de confidencial, por lo que el personal que labore no puede hacer uso de la información de manera personal, tampoco podrá facilitar la información a personal externo

NOTA

Los equipos de cómputo asignados al personal que labore en la organización serán de uso exclusivo por cada funcionario con fines laborales, siendo responsable por los daños de los activos asignado en el manual que se encuentra

Cronograma de actividades

A continuación, se planteó un cronograma de actividades con el fin de gestionar las políticas de seguridad de la información relacionadas en el manual ANEXO 3, serán permeadas a todos los procesos estratégicos, de evaluación, misionales y de apoyo.

CRONOGRAMA DE ACTIVIDADES							
Actividad	Responsable(s)	Mes 1	Mes 2	Mes 3	Mes 4	Mes 5	Mes 6
Formación del Comité Técnico de Seguridad	Autoridades ancestrales, Representante legal, Apoyo técnico	X					
Diagnóstico de infraestructura y activos	Área de sistemas, Comité técnico	X					
Definición y aprobación de políticas generales	Comité técnico, Autoridades ancestrales	X					
Capacitación inicial del personal	Área de sistemas, Comité técnico		X				
Implementación de controles de acceso	Área de sistemas		X				
Configuración de dispositivos móviles y conexión remota	Área de sistemas		X				
Gestión de activos de información	Área de sistemas, Jefes de área			X			
Seguridad física y ambiental	Comité técnico, Área de sistemas			X			
Implementación de copias de seguridad y recuperación	Área de sistemas				X		
Monitoreo y registro de actividades	Área de sistemas				X		
Simulacros de gestión de incidentes	Comité técnico, Área de sistemas					X	
Revisión y ajuste de políticas y procedimientos	Comité técnico, Autoridades ancestrales					X	
Auditoría interna y evaluación final	Comité técnico, Área de sistemas, Autoridades ancestrales						X
Difusión y reforzamiento de la cultura de seguridad	Comité técnico, Autoridades ancestrales						X

A continuación, se hace un resumen de las políticas de seguridad con el fin de garantizar el desarrollo y la aplicabilidad de las políticas de seguridad en la infraestructura tecnológica del cabildo indígena resguardo de Jambaló como se muestra en la Tabla 4. **ANEXO 3**

RESUMEN POLITICAS DE SEGURIDAD	
POLITICAS	CONTENIDO
Política de estructura organizacional de seguridad de la información	Para el cabildo indígena resguardo de Jambaló es muy importante contar con una estructura organizacional de seguridad de la información definida, que permita la acertada toma de decisiones y que garantice la protección de los activos de información de la Organización, se toma como referencia los lineamientos que brinda la norma iso 27001 y las recomendaciones de seguridad de NIST
Política para uso de dispositivos móviles	El cabildo indígena resguardo de Jambalo define las directrices para el uso responsable y manipulación de los dispositivos móviles organizacionales (teléfonos inteligentes y tablets) asignados a las personas que hagan uso de estos activos o servicios de la organización.
Políticas de seguridad de recursos humanos	El cabildo indígena resguardo de jambalo realiza acciones pertinentes para garantizar que la política de confidencialidad y buen uso de los recursos tecnológicos sean incluidos en los contratos o cualquier formato de vinculación laboral y que tengan acceso a las instalaciones físicas y sistemas de información de la Organización.
Política de gestión de activos de la organización.	El cabildo indígena resguardo de jambaló es propietaria de los activos de información físicos (equipos de cómputo tipo servidor, equipos de cómputo tipo estaciones de trabajo, equipos de cómputo tipo portátiles, impresoras, teléfonos, dispositivos de redes, entre otros), los servicios (internet, correo electrónico, aplicaciones), la información (generada, procesada, almacenada y transmitida) y los avances tecnológicos e intelectuales desarrollados por el personal de la Organización , derivados del cumplimiento de las funciones y tareas asignadas.
Políticas de seguridad en acceso de control	El cabildo indígena resguardo de jambalo define las reglas para garantizar la creación, modificación, bloqueo o eliminación de las cuentas de usuario, que permiten el acceso lógico a los recursos tecnológicos y los sistemas de información de la Organización.
Políticas de gestión de copias de seguridad de la información	Asegurar la operación correcta de la información almacenada en los diferentes componentes de los sistemas de información de la organización, que se encuentren debidamente consignados en un lugar seguro permitiendo su respaldo en caso de requerirlo y mitigando el riesgo de pérdida de la información.
Políticas de gestión de claves	El cabildo indígena resguardo de Jambalo define reglas para la generación, distribución, uso, renovación y destrucción de claves
Políticas de seguridad físicas y ambientales	Prevenir el acceso físico no autorizado, por pérdida de daños de la información en la infraestructura tecnológica en el cabildo indígena resguardo de Jambaló y prevenir la alteración por pérdida o daños de los activos a continuación se documentan las políticas de seguridad física y ambiental de la organización.
Políticas de seguridad a Redes inalámbricas	El cabildo resguardo de jambaló define los lineamientos para garantizar que todos los funcionarios que requieran acceder a la red inalámbrica propiedad de la organización, puedan realizar sus actividades con eficiencia y cumpliendo a cabalidad con los directrices estipuladas para garantizar la confidencialidad, integridad y disponibilidad de la información de la Organización.
Política de cumplimiento	Todo el personal que esté vinculado laboralmente en el cabildo debe cumplir con todas las políticas de seguridad y evitar violaciones legales y queda sujeto al cumplimiento obligatorio de las normas expuestas, evitar sanciones o llamados de atención hasta la suspensión o retiro del cargo si es necesario.

Tabla 12 Resumen políticas de seguridad

3.5.1. Políticas de seguridad de la información asociado al control de seguridad

A continuación, se estableció los parámetros de las políticas de seguridad de la información asociado con el control de seguridad lo cual establecen el compromiso de la organización con la protección de sus activos de información, definiendo lineamientos, responsabilidades y procedimientos obligatorios para el manejo seguro de los datos.

CONTROL DE SEGURIDAD INFRAESTRUCTURA TECNOLÓGICA EN EL CABILDO INDÍGENA RESGUARDO DE JAMBALÓ						
Mes	Área / Política	Actividad / Control	Responsable	Fecha Inicio	Estado	Prioridad
1	Estructura Organizacional	Conformación Comité Técnico de Seguridad y asignación de roles	Autoridades ancestrales, Apoyo técnico SI	1/20/2025	No iniciado	Alta
1	Gestión de Activos	Inventario inicial de activos de información y tecnológicos	Área de sistemas		No iniciado	Alta
1	Control de Acceso	Definición de roles, privilegios y políticas de contraseñas	Área de sistemas		No iniciado	Alta
2	Dispositivos Móviles	Configuración y entrega de dispositivos a usuarios	Área de sistemas		No iniciado	Alta
2	Seguridad Física y Ambiental	Evaluación de instalaciones, cableado, sistema eléctrico y mantenimiento de equipos	Área de sistemas, Autoridades ancestrales		No iniciado	Alta
2	Capacitación de personal	Sensibilización en políticas de seguridad	Autoridades ancestrales, Área de sistemas		No iniciado	Alta
3	Gestión de Copias de Seguridad	Implementación de procedimientos de backup y restauración	Área de sistemas		No iniciado	Alta
3	Conexiones Remotas	Configuración segura de acceso remoto y portal cautivo	Área de sistemas		No iniciado	Alta
3	Gestión de Incidentes	Definición de proceso de gestión de incidentes	Área de sistemas, Comité Técnico SI		No iniciado	Alta
4	Gestión de Activos	Procedimientos de entrega y devolución de activos	Área de sistemas, Jefes de área		No iniciado	Alta
4	Comunicaciones y Operaciones	Implementación de antivirus, antispam, monitoreo de eventos	Área de sistemas		No iniciado	Alta
4	Seguridad de Sistemas	Actualización de sistemas operativos, software y antivirus	Área de sistemas		No iniciado	Alta
5	Control de Cumplimiento	Revisión legal y normativa de políticas de seguridad	Comisión jurídica, Autoridades ancestrales		No iniciado	Alta
5	Capacitación Continua	Simulacros de incidentes y entrenamiento	Área de sistemas, Autoridades ancestrales		No iniciado	Alta
6	Auditoría y Revisión	Evaluación de cumplimiento de políticas y controles	Comité Técnico SI, Auditoría interna		No iniciado	Alta
6	Ajustes y Mejora	Actualización de políticas y procedimientos	Comité Técnico SI		No iniciado	Alta

3.5.2. *Análisis y evaluación del Impacto riesgo:*

El análisis de impacto de riesgo es un proceso crucial que se utiliza para garantizar que las políticas sean efectivas y puedan ser mitigados los riesgos en el cabildo indígena resguardo de Jambalo lo cual se estableció la evaluación del impacto potencial de cada amenaza sobre los activos identificados para establecer la probabilidad de ocurrencia mediante el impacto cuantitativo y cualitativo.

A continuación, se establece el impacto de riesgo de seguridad:

Análisis y evaluación del Impacto riesgo		
impacto	impacto cuantitativo	impacto cualitativo
bajo	Pérdida mínima de datos o funciones, recuperable con poco esfuerzo en la organizacion.	no afecta la imagen de la organización y genera reprocesos menores que se puede recuperar
moderado	Pérdidas moderadas de datos o funciones, recuperable con esfuerzo considerable	afecta el desarrollo moderado de la seguridad se puede recuperar la informacion de la organizacion pero de poca calidad
alto	Pérdida crítica de datos o funciones, difícil o imposible de recuperar.	afecta la imagen de la organización no se puede recuperar financieremente y afecta la seguridad de la informacion

3.5.3. Evaluación de la Probabilidad

En la evaluar de la probabilidad de ocurrencia en el cabildo indigena resguardo de Jambalo de acuerdo a los riesgos establecidos

• Probabilidad Baja: Rara vez ocurre.
• Probabilidad Moderada: Ocurre ocasionalmente
• Probabilidad Alta: Ocurre con frecuencia.

3.5.4. Clasificación de evaluación de riesgo

la clasificación de evaluación de riesgo se utiliza para identificar, analizar y priorizar el riesgo para tomar decisiones sobre las medidas de seguridad, estimando el impacto y la probabilidad de tolerancia para buscar nuevas estrategias o controles pertinentes.

CLASIFICACIÓN EVALUACIÓN DE RIESGO			
Impacto	Probabilidad		
	Bajo	Moderado	Alto
bajo	Bajo	Moderado	Moderado
Moderado	Moderado	Moderado	Alto
Alto	Moderado	alto	Alto

3.5.5. Plan de tratamiento de Riesgos

El plan de tratamiento de riesgo en el cabildo indigena resguardo de Jambalo busca gestionar y mitigar los riesgos identificados, especialmente aquellos que pueden afectar la seguridad de los activos de informacion.

A continuación, se presenta los principales riesgos que afectan la organización.

PLAN DE TRATAMIENTO RIESGO CABILDO INDIGENA RESGUARDO JAMBALO							
AMENAZAS	ACTIVOS	riesgo inicial o inherente		Probabilidad	Riesgo	Medidas de mitigación de riesgo	Control
		cuantitativo	calitativo				
Desconocimiento en seguridad de la información	informacion		Alto	Alto	Alto	Dar cumplimiento con los acuerdo de diligenciamiento de confidencialidad para todos los empleados	A.5.1.1 Políticas para la seguridad de la información A. 5.1.2 Revisión de la política
Falta de capacidad para asignar funciones específicas en seguridad de la información	Talento Humano		Moderado	Moderado	Moderado	definir y asignar claramente las responsabilidades de seguridad de la información dentro de una organización	6.1.1 Asignación de responsabilidades para la segur. de la información.
Funcionarios con desconocimiento en temas de contratación de personal Cambios en las regulaciones y lineamientos del gobierno que puedan impactar las operaciones de la organización Insuficiente protección y privacidad de información personal	informacion y Talento Humano		Alto	Alto	Alto	Verificar la veracidad de los antecedentes de los funcionarios que esté acorde a las funciones u obligaciones laborales . Validar procedimiento de vinculación y retiro laboral desde las áreas pertinentes y capacitar al personal en seguridad de la información para concientizar en buen manejo de seguridad	7.2.2 Concienciación, educación y capacitación en segur. de la información A.7.1.1 Selección de condiciones del empleo A.7.2.3 Proceso disciplinario A.7.3.1 Responsabilidades en la terminación o cambio del empleo.
perdida de equipos	area administrativas	Moderado		Moderado	Moderado	Todos los empleados y usuarios de partes externas deberían devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	8.1.4 Devolución de activos.
Acceso no autorizado	administracion de informacion en los equipos de computo bases de datos	Alto		Moderado	Alto	planes de control control de usuarios	9.4.3 Gestión de contraseñas de usuario.
Robo o hurto de información catalogada como sensible por falta de implementación de herramientas que aseguren el transporte de la información por la red	Informacion		Alto	Alto	Alto	Implementación de controles criptográficos y gestión de llaves criptográficas	A.10.1.1 Política sobre el uso de controles criptográficos
desastres naturales	daños por incendios de Informacion, Hardware software	Moderado		Alto	Alto	Respaldo de informacion copias de seguridad	11.1.4 Protección contra las amenazas externas y ambientales
indisponibilidad de fluido eléctrico en el centro de datos y PCs	Informacion, Hardware software	Moderado		Alto	Alto	Realizar inspecciones periódicas de los equipos tecnológicos y de respaldo (servidores, UPS, planta eléctrica) para verificar su funcionamiento y ejecutar las correcciones necesarias	A.11.2.2 Servicios de suministro
estructuración del cableado red	red LAN	Alto		Moderado	Moderado	adecuación de cableado	11.2.3 Seguridad del cableado
Falla en el Hardware	equipo de computo	Moderado		Bajo	Moderado	mantenimientos preventivos	11.2.4 Mantenimiento de los equipos.
Afectación en la disponibilidad del respaldo de la información. Insuficiencia de espacio o almacenamiento para el aseguramiento de la información. Pérdida o corrupción de los datos.	informacion		Alto	Alto	Alto	política y procedimientos para la realización de backups a software, imágenes de los sistemas operativos, e información crítica Verificación de las copias de respaldo por medio de pruebas de restauración	12.3.1 Copias de seguridad de la información.
Fuga o pérdida de información generada por código malicioso. Divulgación no autorizada de información debido a acceso de terceros a través del uso de malware. Indisponibilidad de la información generada por virus informáticos.	Informacion, Hardware software		Alto	Moderado	Alto	Establecer e implementar políticas para la gestión de vulnerabilidades técnicas y para la restricción de instalación de software en sistemas operativos	A.12.6.2 Restricciones sobre la instalación de software

3.5.5.1. Estimación de un presupuesto global

Para el desarrollo del proyecto se tiene una estimación de 3.300.000 millones, los cuales los recursos son propios sin ánimo de lucro se busca es aportar al fortalecimiento en seguridad de la información en el cabildo indígena resguardo de Jambaló.

ESTIMACIÓN DE UN PRESUPUESTO GLOBAL

RUBROS	Fuentes			
	Recurso s propios	Convoca toria interna	Contrapar tida externa	Total
Horas de trabajo	500000	0	0	500000
Horas de asesoria	0	0	0	0
Equipos de computo	2000000	0	0	2000000
Servicio de internet	400000	0	0	400000
Bibliografia	0	0	0	0
Otros	400000			400000
Total	3300000	0	0	3300000

Tabla 13 Estimación de costo

CAPÍTULO 4

4. RESULTADOS ALCANZADOS

En este capítulo se recopila las soluciones planteadas para el diseño una propuesta metodológica para la gestión de la seguridad de la información en la infraestructura tecnológica en el cabildo indígena resguardo de Jambaló, resumiendo los avances logrados en cada una de las etapas del proyecto.

Con el diseño una propuesta metodológica para la gestión de la seguridad de la información en la infraestructura tecnológica en el cabildo indígena resguardo de Jambaló, se logró identificar y hacer el inventario de los activos de la información, conocer el estado actual de la organización indígena en materia de seguridad.

A continuación, se presenta los resultados alcanzados

- ✓ Identificación e inventario de activos
- ✓ Plan de tratamiento de riesgo
- ✓ Contingencia de control de seguridad
- ✓ Mitigación y mejoras resultados diseño una propuesta metodológica para la gestión de la seguridad de la información en la infraestructura tecnológica en el cabildo indígena resguardo de Jambalo.
- ✓ Diseño y presentación de la propuesta del sistema de gestión de seguridad a la Autoridades ancestrales

4.1. Identificación e inventario de activos

Se realizó la identificación de los principales activos de la información y el diagnóstico actual de la infraestructura tecnológica en el cabildo indígena resguardo de Jambaló en cada visita se logró identificar las posibles fallas de seguridad en los que están incurriendo actualmente en el mal uso de los activos. En el ANEXO 1 se realizó el inventario de activos.

4.2. Plan de tratamiento riesgo

Se identificaron los posibles riesgos y conocer las debilidades que tiene la infraestructura tecnológica en el cabildo indígena resguardo de Jambaló en seguridad de gestión, a continuación, se realizó el tratamiento de las políticas de seguridad

CONTROL DE SEGURIDAD INFRAESTRUCTURA TECNOLÓGICA EN EL CABILDO INDIGENA RESGUARDO DE JAMBALÓ								
Mes	Área / Política	Actividad / Control	Responsable	Fecha Inicio	Fecha Fin	Estado	Evidencia / Observaciones	Prioridad
1	Estructura Organizacional	Conformación Comité Técnico de Seguridad y asignación de roles	Autoridades ancestrales, Apoyo técnico SI	1/20/2025	5/1/2025	Finalizado	Acta de conformación del comité	Bajo
1	Gestión de Activos	Inventario inicial de activos de información y tecnológicos	Área de sistemas	2/2/2025	5/1/2025	Finalizado	Inventario físico y digital	Bajo
1	Control de Acceso	Definición de roles, privilegios y políticas de contraseñas	Área de sistemas	2/5/2025	5/1/2025	Finalizado	Documento aprobado por comité	Moderado
2	Dispositivos Móviles	Configuración y entrega de dispositivos a usuarios	Área de sistemas	2/23/2025	5/1/2025	Finalizado	Registro de entrega y configuración	Moderado
2	Seguridad Física y Ambiental	Evaluación de instalaciones, cableado, sistema eléctrico y mantenimiento de equipos	Área de sistemas, Autoridades ancestrales	2/24/2025	5/1/2025	Finalizado	Informe de evaluación	Moderado
2	Capacitación de personal	Sensibilización en políticas de seguridad	Autoridades ancestrales, Área de sistemas	2/25/2025	5/1/2025	Iniciado	Lista de asistencia, evidencias de capacitación	Moderado
3	Gestión de Copias de Seguridad	Implementación de procedimientos de backup y restauración	Área de sistemas	3/26/2025	5/1/2025	Iniciado	Procedimiento documentado	Moderado
3	Conexiones Remotas	Configuración segura de acceso remoto y portal cautivo	Área de sistemas	3/27/2025	5/1/2025	Iniciado	Reporte de configuración	Alta
3	Gestión de Incidentes	Definición de proceso de gestión de incidentes	Área de sistemas, Comité Técnico SI	3/28/2025	5/1/2025	Iniciado	Procedimiento y plantilla de reporte	Alta
4	Gestión de Activos	Procedimientos de entrega y devolución de activos	Área de sistemas, Jefes de área	4/2/2025	5/1/2025	Iniciado	Paz y salvo firmado	Moderado
4	Comunicaciones y Operaciones	Implementación de antivirus, antispam, monitoreo de eventos	Área de sistemas	4/15/2025	5/1/2025	No iniciado	Informes de configuración	Alta
4	Seguridad de Sistemas	Actualización de sistemas operativos, software y antivirus	Área de sistemas	31/4/2025	5/1/2025	Iniciado	Checklist de actualizaciones	Moderado
5	Control de Cumplimiento	Revisión legal y normativa de políticas de seguridad	Comisión jurídica, Autoridades ancestrales	4/1/2025	5/1/2025	No iniciado	Informe de cumplimiento	Alta
5	Capacitación Continua	Simulacros de incidentes y entrenamiento	Área de sistemas, Autoridades ancestrales	5/1/2025	5/1/2025	No iniciado	Registro de simulacros	Alta
6	Auditoría y Revisión	Evaluación de cumplimiento de políticas y controles	Comité Técnico SI, Auditoría interna	5/1/2025	5/1/2025	Iniciado	Informe final y plan de mejora	Alta
6	Ajustes y Mejora	Actualización de políticas y procedimientos	Comité Técnico SI	5/1/2025	5/1/2025	No iniciado	Políticas revisadas y aprobadas	Alta

PLAN DE TRATAMIENTO RIESGO CABILDO INDIGENA RESGUARDO JAMBALO							
AMENAZAS	ACTIVOS	Riesgo residual		Probabilidad	Evaluación	Medidas de mitigación de riesgo	Control
		Impacto cuantitativo	Impacto cualitativo				
Desconocimiento en seguridad de la información	información		Moderado	Moderado	Moderado	Dar cumplimiento con los acuerdos de diligenciamiento de confidencialidad para todos los empleados	A.5.1.1 Políticas para la seguridad de la información A. 5.1.2 Revisión de la política
Falta de capacidad para asignar funciones específicas en seguridad de la información	Talento Humano		Bajo	Bajo	Bajo	definir y asignar claramente las responsabilidades de seguridad de la información dentro de una organización	6.1.1 Asignación de responsabilidades para la segur. de la información.
Funcionarios con desconocimiento en temas de contratación de personal Cambios en las regulaciones y lineamientos del gobierno que puedan impactar las operaciones de la organización Insuficiente protección y privacidad de información personal	información y Talento Humano		Moderado	Moderado	Moderado	Verificar la veracidad de los antecedentes de los funcionarios que esté acorde a las funciones u obligaciones laborales. Validar procedimiento de vinculación y retiro laboral desde las áreas pertinentes y capacitar al personal en seguridad de la información para concientizar en buen manejo de seguridad	7.2.2 Concienciación, educación y capacitación en segur. de la información A.7.1.1 Selección A.7.1.2 Términos y condiciones del empleo A.7.2.3 Proceso disciplinario A.7.3.1 Responsabilidades en la terminación o cambio del empleo.
perdida de equipos	area administrativas			Bajo	Bajo	Todos los empleados y usuarios de partes externas deberían devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	8.1.4 Devolución de activos.
Acceso no autorizado	administración de información en los equipos de computo bases de datos	Alto		Moderado	Alto	planes de control control de usuarios	9.4.3 Gestión de contraseñas de usuario.
Robo o hurto de información catalogada como sensible por falta de implementación de herramientas que aseguren el transporte de la información por la red	Información		Moderado	Alto	Alto	Implementación de controles criptográficos y gestión de claves criptográficas	A.10.1.1 Política sobre el uso de controles criptográficos
desastres naturales	daños por incendios de Información, Hardware software	Moderado		Moderado	Moderado	Respaldo de información copias de seguridad	11.1.4 Protección contra las amenazas externas y ambientales
Indisponibilidad de fluido eléctrico en el centro de datos y PCs	Información, Hardware software	Moderado		Moderado	Moderado	Realizar inspecciones periódicas de los equipos tecnológicos y de respaldo (servidores, UPS, planta eléctrica) para verificar su funcionamiento y ejecutar las correcciones necesarias	A.11.2.2 Servicios de suministro
estructuración del cableado red	red LAN	Moderado		Moderado	Moderado	adecuación de cableado	11.2.3 Seguridad del cableado
Falla en el Hardware	equipo de computo	Bajo		Bajo	Bajo	mantenimientos preventivos	11.2.4 Mantenimiento de los equipos.
Afectación en la disponibilidad del respaldo de la información. Insuficiencia de espacio o almacenamiento para el aseguramiento de la información. Pérdida o corrupción de los datos.	Información		Moderado	Moderado	Moderado	política y procedimientos para la realización de backups a software, imágenes de los sistemas operativos, e información crítica Verificación de las copias de respaldo por medio de pruebas de restauración	12.3.1 Copias de seguridad de la información.
Fuga o pérdida de información generada por código malicioso. Divulgación no autorizada de información debido a acceso de terceros a través del uso de malware. Indisponibilidad de la información generada por virus informáticos.	Información, Hardware software		Alto	Moderado	Alto	Establecer e implementar políticas para la gestión de vulnerabilidades técnicas y para la restricción de instalación de software en sistemas operativos	A.12.6.2 Restricciones sobre la instalación de software

4.3. Evaluación de la Probabilidad

En la evaluar de la probabilidad de ocurrencia en el cabildo indígena resguardo de Jambalo de acuerdo a los riesgos establecidos

• Probabilidad Baja: Rara vez ocurre.
• Probabilidad Moderada: Ocurre ocasionalmente
• Probabilidad Alta: Ocurre con frecuencia.

4.4. Nivel de riesgo

Para evaluar el mapa de riesgo de la tabla plan de tratamiento de riesgo se hace un diagnóstico de la cantidad de evaluación al cumplimiento de los controles respectivos.

Nivel	Cantidad
Bajo	3
Moderado	6
Alto	3
Extremo	0

4.5. Mapa residual de riesgo

Para establecer el mapa de riesgo se mira la probabilidad respecto al impacto de riesgo que puede tener la organización frente métricas establecidas.

Mapa de Riesgo Residual				
PROBABILIDAD	IMPACTO			
	1 a 2- BAJO	3- MODERADO	4-ALTO	5- CATASTR OFICO
4 a 5 -ALTO				
3-MODERADO				
1 a 2 -BAJO				

4.6. Contingencia de control de seguridad

Se realizo el plan de contingencia de los riesgos residuales de acuerdo al tratamiento de los controles establecidos lo que garantiza la eficacia del diseño una propuesta metodológica para la gestión de la seguridad de la información en la infraestructura tecnológica en el cabildo indígena resguardo de Jambaló, así mismo se puede constatar la disminución de los riesgos iniciales con la implementación de las políticas de seguridad en la organización indígena lo cual garantiza la confidencialidad, integridad y disponibilidad de los datos.

Control			
Contingencia	Control	residual	Riesgo
El departamento jurídico de la organización en conjunto con las autoridades ancestrales debe redactar un documento de confidencialidad en el que obliga al empleado de no divulgar información ni activos de la organización, este documento debe ser firmado antes de la contratación y archivado junto con la hoja de vida	Dar cumplimiento con los acuerdo de diligenciamiento de confidencialidad para todos los empleados	A.5.1.1 Políticas para la seguridad de la información A. 5.1.2 Revisión de la política	Moderado
Las autoridades ancestrales deben validar la información suministrada por el empleado antes de la contratación, revisar sus antecedentes y explicar los deberes y responsabilidades de seguridad.	definir y asignar claramente las responsabilidades de seguridad de la información dentro de una organización	6.1.1 Asignación de responsabilidades para la segur. de la información.	Bajo
Las autoridades ancestrales deben validar la información suministrada para la veracidad de los antecedentes	Verificar la veracidad de los antecedentes de los funcionarios que esté acorde a las funciones u obligaciones laborales Validar procedimiento de vinculación y retiro laboral desde las áreas pertinentes y capacitar al personal en seguridad de la información para concientizar en buen manejo de seguridad	7.2.2 Concienciación, educación y capacitación en segur. de la información A.7.1.1 Selección A.7.1.2 Términos y condiciones del empleo A.7.2.3 Proceso disciplinario A.7.3.1 Responsabilidades en la terminación o cambio del empleo.	Moderado
El personal que sea retirado o removido del cargo deberá devolver en perfecto estado los equipos tecnológicos al encargado de sistemas	Todos los empleados y usuarios de partes externas deberían devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	8.1.4 Devolución de activos.	Bajo
Si el usuario es bloqueado deberá ser desbloqueado por el área de seguridad encargada, en caso de que el usuario se bloquee deberá esperar a que sea habilitado, no se permite el préstamo de usuarios	planes de control	9.4.3 Gestión de contraseñas de usuario.	Alto
	control de usuarios		
Asignar roles y privilegios de acceso de acuerdo con las responsabilidades de cada usuario.	Implementación de controles criptográficos y gestión de llaves criptográficas	A.10.1.1 Política sobre el uso de controles criptográficos	Alto
Implementar herramientas de monitoreo de eventos y registros de actividad para detectar posibles amenazas o incidentes	Respaldo de información	11.1.4 Protección contra las amenazas externas y ambientales	Moderado
	copias de seguridad		
Realizar copias de seguridad periódicas de la información crítica y almacenarlas en un lugar seguro.	Realizar inspecciones periódicas de los equipos tecnológicos y de respaldo (servidores, UPS, planta eléctrica) para verificar su funcionamiento y ejecutar las correcciones necesarias	A.11.2.2 Servicios de suministro	Moderado
Solo en personal de sistemas es el encargado de realizar el mantenimiento de los equipos de compute	mantenimientos preventivos	11.2.4 Mantenimiento de los equipos.	Bajo
Los usuarios podrán hacer uso de los diferentes medios de almacenamiento en la nube dado por la organización y facilite el procesamiento de la información, en la medida que cumplan las políticas de seguridad establecidas para prevenir la propagación de virus o código malicioso.	política y procedimientos para la realización de backups a software, imágenes de los sistemas operativos, e información crítica Verificación de las copias de respaldo por medio de pruebas de restauración	12.3.1 Copias de seguridad de la información.	Moderado
el area de sistema debe restringir la instalacion de software no autorizado para prevenir riesgo de malware solose puede instalar software autorizados	Establecer e implementar políticas para la gestión de vulnerabilidades técnicas y para la restricción de instalación de software en sistemas operativos	A.12.6.2 Restricciones sobre la instalación de software	Alto

Tras hacer el plan de tratamiento de riesgo inicial y el residual se puede constatar que el nivel de riesgo es menor lo cual la propuesta es viable y garantiza la protección de los activos del cabildo indígena resguardo de Jambalo.

4.7. Mitigación y mejoras resultados diseño una propuesta metodológica para la gestión de la seguridad de la información en la infraestructura tecnológica en el cabildo indígena resguardo de Jambalo.

Gracias al desarrollo y a los resultados alcanzados con diseño de gestión de seguridad en el cabildo indígena resguardo de jambalo se logró alcanzar.

A continuación, logros alcanzados de la implementación de las políticas de seguridad:

1. Se logro que el cabildo indígena adquirir e implemente dominio cabildojambalo.org y la configuración de Google Workspace para organizaciones sin ánimo de lucro, con el fin de manejar correos corporativos para sus empleados, y así mejoras la seguridad de la informacion esto marca un hito importante en el fortalecimiento de la infraestructura tecnológica del Cabildo de Jambaló.

Estas acciones permiten:

- ✓ Mejorar la comunicación interna y externa de la organización. Consolidar la presencia digital del Cabildo, aumentando su visibilidad y credibilidad
- ✓ Garantizar herramientas tecnológicas modernas para la gestión de proyectos y actividades diarias. ya que no contaban con correos corporativos y sus empleados utilizabas sus cuentas personales para guardar informacion

- ✓ Maquetación de activos: Se realizó maquetación de los aparatos tecnológicos para evitar pérdida de activos

4.8. Diseño y presentación de la propuesta del sistema de gestión de seguridad a la Autoridades ancestrales

Se presentó a las autoridades ancestrales del cabildo indígena resguardo de Jambaló la propuesta metodológica para la gestión de la seguridad de la información en la cual se logró la aprobación e implementación del sistema de gestión seguridad.

Se diseñó el manual de las políticas de seguridad para la infraestructura tecnológica en el cabildo indígena resguardo de Jambaló, se tomó como referencia la normatividad de la ISO 27001 y los estándares internacionales de la NIST para establecer las diferentes políticas y controles de seguridad. En el ANEXO 3 se encuentran las políticas de seguridad y en el ANEXO 4 los controles de seguridad

4.9. Certificación y aval de la implementación del sistema de gestión de seguridad.

Para garantizar el cumplimiento de la aprobación e implementación del diseño una propuesta metodológica para la gestión de la seguridad de la información en la infraestructura tecnológica en el cabildo indígena resguardo de Jambaló las autoridades ancestrales aval la implementación en la cual se hizo entrega.

- ✓ Manual de políticas de seguridad
- ✓ Proyecto de grado.

En los anexos se adjunta el aval del cabildo de la implementación del proyecto de grado

ANEXO 5

CAPÍTULO 5

5. CONCLUSIONES

Al terminar este proyecto, se concluye que los sistemas de gestión de la seguridad de la información es un factor fundamental que permiten tener buenas prácticas de seguridad y prevenir sobre los falla o riesgos que afectan los activos y la información de la organización además afecta la disponibilidad, la confidencialidad y la integridad de la información.

Con el desarrollo de este proyecto, logró identificar la situación actual de la organización indígena, los riesgos de seguridad. Permitiendo diseñar una propuesta metodológica para la gestión de la seguridad de la información en la infraestructura tecnológica en el cabildo indígena resguardo de Jambaló ajustando todos los hallazgos y permitiendo crear las políticas y los controles pertinentes.

Con la realización de este proyecto, se logra la permanencia y el crecimiento de la organización utilizando las buenas prácticas de seguridad.

5.1. Trabajos a futuro

Se espera que en un futuro se pueda implementar otros proyectos basados a esta gran experiencia y las organizaciones indígenas puedan desarrollar las buenas prácticas de seguridad de la información tomando como referencia la implementación de un modelo para la gestión de la seguridad de la información en la infraestructura tecnológica en el Cabildo Indígena, Resguardo de Jambaló.

BIBLIOGRAFÍA

International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. ISO.

INFOBAE. (2021, 2 de julio). En el 2021 aumentaron en un 30% los ciberataques en Colombia . infobae. <https://www.infobae.com/america/colombia/2021/07/02/en-el-2021-aumentaron-en-un-30-los-ciberataques-en-colombia/>

Estudio trimestral de ciberseguridad: Ataques a entidades de gobierno. (2022, April 6). CCIT - Cámara Colombiana de Informática y Telecomunicaciones; Cámara Colombiana de Informática y Telecomunicaciones. <https://www.ccit.org.co/estudios/estudio-trimestral-de-ciberseguridad-ataques-a-entidades-de-gobierno/>

OSPINA DIAZ, Milton Ricardo and SANABRIA RANGEL, Pedro Emilio.Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. Rev. Crim. [online]. 2020, vol.62, n.2, pp.199-217. Epub Nov 26, 2020. ISSN 1794-3108.

Vergara Torres, & Horacio, O. (2019). Mejorando la implantación de la ISO 27001 en las organizaciones. <http://repository.unipiloto.edu.co/handle/20.500.12277/6178>

Balance de Ciberseguridad 2024: Desafíos y prevención para un entorno digital seguro . (2025, 28 de marzo). CCIT - Cámara Colombiana de Informática y Telecomunicaciones; Cámara Colombiana de Informática y Telecomunicaciones. <https://www.ccit.org.co/noticias/balance-de-ciberseguridad-2024-desafios-y-prevencion-para-un-entorno-digital-seguro/>

¿Cuáles son los 10 casos de ciberataques más reconocidos en Colombia? (2025, mayo 21). Edu.co. <https://virtual.uao.edu.co/blog/cuales-son-los-10-casos-de-ciberataques-mas-reconocidos-en-colombia>

Forbes Colombia.

<https://forbes.co/2024/02/28/tecnologia/colombia-es-el-pais-con-mas-ataques-de-ciberseguridad-en-latinoamerica>

Whitman, M., & Mattord, H. (2022). *Principles of information security* (7th ed.). Cengage Learning.

International Organization for Standardization. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. ISO.

González, M., & Ramírez, P. (2021). *Gestión de la seguridad de la información en entornos organizacionales*. *Revista Colombiana de Informática*, 13(2), 55–68.

International Organization for Standardization. (2018). *ISO 31000:2018 Risk management — Guidelines*. ISO.

Camargo, Erney Alberto Ramírez, & Pinzon, Miguel Alberto Rinconc. (2022). *La importancia de la seguridad de la información en el sector público en Colombia.. RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, (46), 97-99. Epub 30 de junho de 2022.<https://doi.org/10.17013/risti.46.87-99>

Ramírez, C., & López, J. (2020). *Aplicación de la gestión de riesgos en comunidades rurales: un enfoque desde la ISO 31000*. *Revista Latinoamericana de Gestión Comunitaria*, 7(1), 33–49.

Actualización del Estándar ISO 27001, versión 2022. (2022, 14 de octubre). Grupo Cynthus . <https://www.cynthus.com.mx/actualizacion-del-estandar-iso-27001/>

¿QUIENES SOMOS? (s/f). *Proyectoglobajambalo.org* de <https://proyectoglobajambalo.org/nosotros/>

Mesa Guzmán, L., María, A., Crowdstrike, & Cruz, P. (s/f). *Equipo TicTac Dirección de desarrollo de programas*: <https://www.ccit.org.co/wp-content/uploads/informe-safe-tendencias-del-ciberdelincuencia-2021-2022.pdf>

Decreto 1078 de 2015 Sector de Tecnologías de la Información y las Comunicaciones - Gestor Normativo. (s. f.). *Función Pública*. <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=77888>

Castro Santana, Carmen Lizbet, León Robaina, Rosario, & Estrada Hernández, José Armando. (2024). *Metodología de gestión de riesgo basado en la Norma ISO 31000*. *Economía y Desarrollo*, 168(2), . Epub 18 de junio de 2024. de http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S0252-85842024000200011&lng=es&tlng=es.

Del, N. (s/f). SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SGSI - MINTIC. Gov.co. https://www.mintic.gov.co/portal/715/articles-135830_plan_tratamiento_seguridad_2020_u20201228.pdf

J. Matiz y M. Rueda, (2020). « Trabajo de Grado Diseño de un modelo de seguridad y privacidad de la información para las empresas de empleo temporal basado en la norma ISO 27001» Universidad Catolica de Colombia, Bogota, 2020.

Informe SAFE - Tendencias del Cibercrimen 2021 - 2022: <https://www.ccit.org.co/wp-content/uploads/informe-safe-tendencias-del-cibercrimen-2021-2022.pdf>

Guzman, P. K. ISO 27001 | Altaos Grupo. Cumplimiento normativo. SGSI. Altaos Grupo. Cumplimiento Normativo. SGSI. https://www.altaosgrupo.com/iso_27001/.

ANEXOS

ANEXO 1. INVENTARIO DE LOS ACTIVOS

ANEXO 2. ANÁLISIS DE RIESGO

**ANEXO 3. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA
INFRAESTRUCTURA TECNOLÓGICA EN EL CABILDO INDÍGENA RESGUARDO
DE JAMBALÓ.**

ANEXO 4. CONTROLES DE SEGURIDAD

ANEXO 5. AVAL

ANEXO 1

Inventario de los activos

El cabildo indígena resguardo de jambaló desde su creación hasta la actualidad cuenta con los siguientes activos.

inventario de activos de la informacion en el cabildo indigena de jambalo			
Nombre de activo	Descripcion de activo	Tipo de activo	Contenedor
Red wifi	Red wifi utilizado por los equipo de la organizacion indigena	Infraestructura del cabildo	Red LAN
Computadores	Computadores asignados a los colaboradores del cabildo	Equipos de computo	Computadores
Portatiles	Portatiles asignados a los colaboradores del cabildo	Equipos de computo	Portatiles
Camara de seguridad	Camaras de seguridad que se encuentran dentro de la organizacion	Equipos de seguridad	Camara de seguridad
Dispositivos de red	Dispositivos activos en el cabildo (switch,router)	Equipos de computo	switch,router
Pagina web	Pagina web del cabildo	Software	Servidores de aplicación
intranet	Pagina web del cabildo	Software	Servidores de aplicación
Bases de datos	bases de datos que utiliza el cabildo	Servicios	Bases de datos



Esta tabla es un diagnóstico del inventario de activos en la Infraestructura Tecnológica en el Cabildo Indígena, Resguardo de Jambaló, para llevar un control básico de los activos gestionados, así como de sus responsables, ubicación, y otras características relevantes.

La descripción de los campos es la siguiente:

- * **Cantidad:** cantidad del activo. que estan en cada oficina
- * **Responsable:** Nombre del responsable del activo. Se puede tratar de una persona concreta o de un departamento.
- * **Tipo:** El campo tipo se utiliza para clasificar los activos. Resulta conveniente distinguir si el activo es físico o si es lógico (intangible).
- * **Ubicación:** Indica dónde está ubicado físicamente el activo.
- * **Crítico:** Campo que indica si el activo juega un papel fundamental / imprescindible (crítico) para la organización.

INVENTARIO DE ACTIVOS				
cantidad	Tipo	Responsable	Ubicación	Crítico
1	computador mesa (físico)	Cordinador Nucleo de salud	oficina nucleo de salud	Sí
1	Switch	Cordinador Nucleo de salud	oficina nucleo de salud	Sí
1	computador mesa (físico)	Secretaria	oficina secretaria general	Sí
1	Impresora	Secretaria	oficina secretaria general	Sí
1	computador mesa (físico)	Encargado del Archivo	oficina de archivo	Sí
1	Impresora	Encargado del Archivo	oficina de archivo	Sí
7	computador mesa (físico)	Tesoreria	oficina de tesoreria	Sí
1	Impresora	Tesoreria	oficina de tesoreria	Sí
1	Switch	Tesoreria	oficina de tesoreria	Sí

1	Camara de seguridad	Tesoreria	oficina de tesoreria	Sí
2	computador mesa (físico)	comision Juridica	oficina comusion juridica	Sí
1	Switch	comision Juridica	oficina comusion juridica	Sí
1	Impresora	comision Juridica	oficina comusion juridica	Sí
3	computador mesa (físico)	Cordinado Nucleo Economico	oficina nucleo economico	Sí
1	Impresora	Cordinado Nucleo Economico	oficina nucleo economico	Sí
1	Switch	Cordinado Nucleo Economico	oficina nucleo economico	Sí
1	computador mesa (físico)	Guardia	oficina de la guardia	Sí
9	Camara de seguridad	Guardia	oficina de la guardia	Sí
2	computador mesa (físico)	P GLOB	oficina P GLOB	Sí
1	Impresora	P GLOB	oficina P GLOB	Sí
1	computador mesa (físico)	Autoridades ancestrales	oficina Autoridades ancestrales	Sí
1	Impresora	Autoridades ancestrales	oficina Autoridades ancestrales	Sí
5	Portatiles	Autoridades ancestrales	oficina Autoridades ancestrales	Sí
1	computador mesa (físico)	Representante Legal	oficina representante legal	Sí
1	Impresora	Representante Legal	oficina representante legal	Sí
5	computador mesa (físico)	cordinador semillas de vida	oficina semillas de vida	Sí
1	Router	cordinador semillas de vida	oficina semillas de vida	Sí
1	Impresora	cordinador semillas de vida	oficina semillas de vida	Sí
7	computador mesa (físico)	Cordinado Nucleo Educcion	oficina nucleo de educacion	Sí
1	Impresora	Cordinado Nucleo Educcion	oficina nucleo de educacion	Sí
1	Router	Cordinado Nucleo Educcion	oficina nucleo de educacion	Sí
2	computador mesa (físico)	Lenguas	oficina de Lenguas	Sí
1	Impresora	Lenguas	oficina de Lenguas	Sí
2	computador mesa (físico)	Mais planeacion-fondo	oficina Mais	No
1	Router	Auditorio	Auditorio	No
7	computador mesa (físico)	Cordinador de comunicaci3n	oficina emisora	No
1	computador mesa (físico)	PEC	oficina PEC	No
1	Impresora	PEC	oficina PEC	No

Diagnóstico estructurado TI

Se realizó un diseño de la estructuración física de la tecnología de la información del cabildo indígena resguardo de Jambaló de sus diferentes oficinas que manejan.

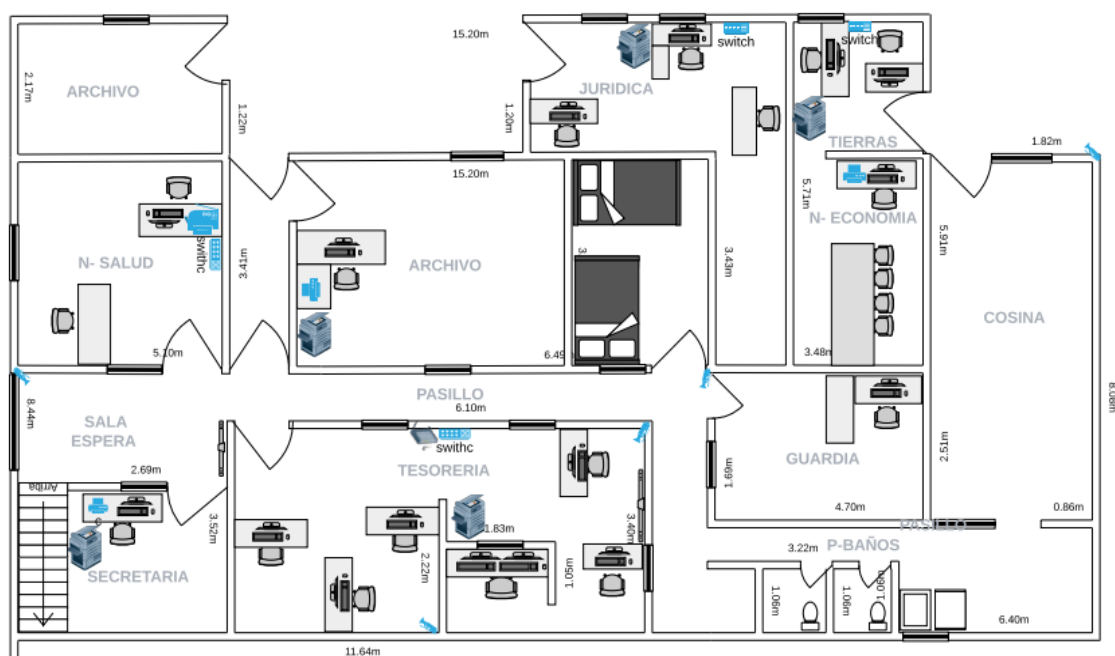


Figura 5 Piso Área administrativas

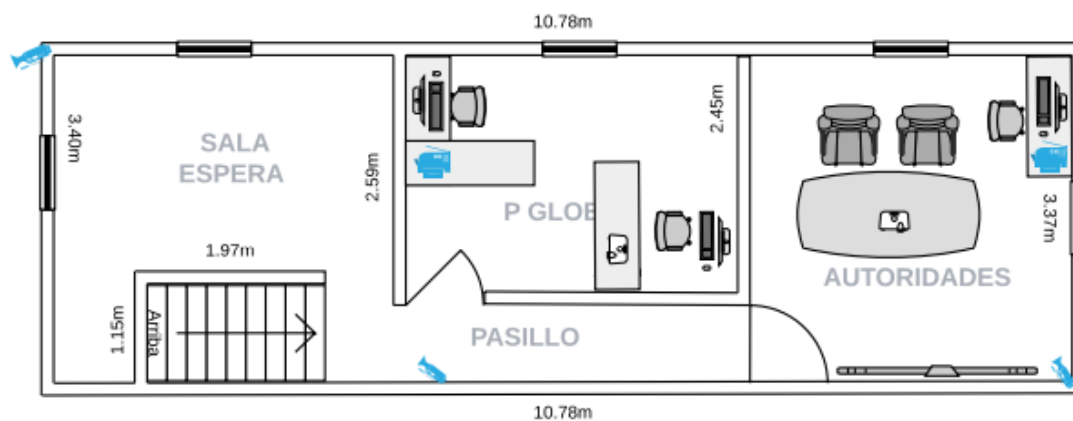


Figura 6 2 Piso Autoridades Ancestrales

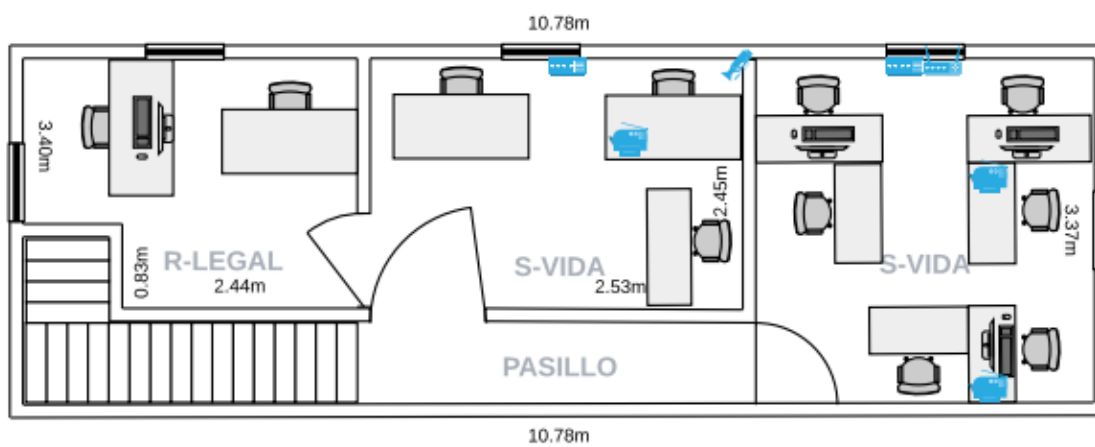


Figura 7 3 Piso Representante Legal

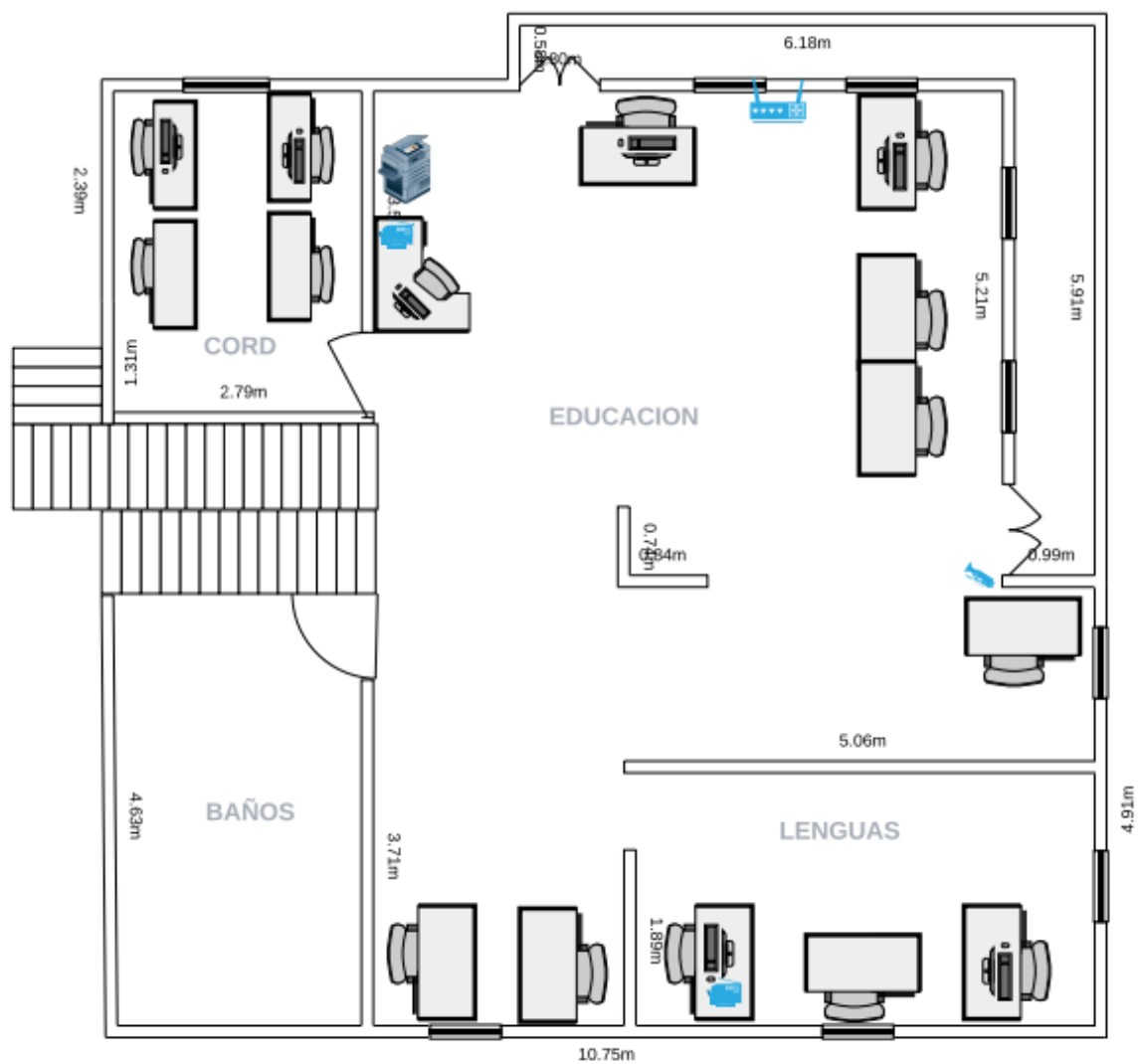


Figura 8 2 piso Núcleo de Educación

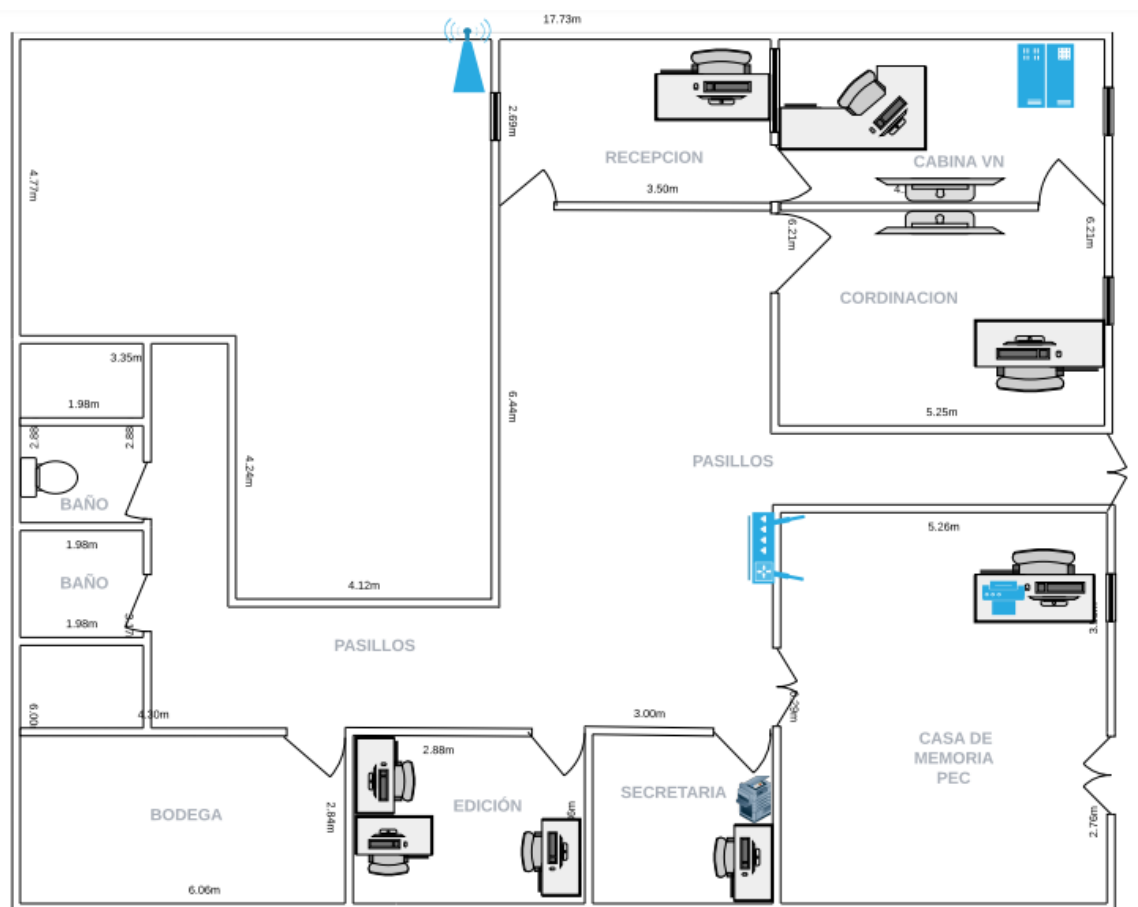


Figura 10 Emisora Comunitaria

ANEXO 2

ANÁLISIS DE RIESGO

CONTROL DE SEGURIDAD INFRAESTRUCTURA TECNOLÓGICA EN EL CABILDO INDIGENA RESGUARDO DE JAMBALÓ								
Mes	Área / Política	Actividad / Control	Responsable	Fecha Inicio	Fecha Fin	Estado	Evidencia / Observaciones	Prioridad
	Estructura Organizacional	Conformación Comité Técnico de Seguridad y asignación de roles	Autoridades ancestrales, Apoyo técnico SI	1/20/2025	5/1/2025	Finalizado	Acta de conformación del comité	Bajo
1	Gestión de Activos	Inventario inicial de activos de información y tecnológicos	Área de sistemas	2/2/2025	5/1/2025	Finalizado	Inventario físico y digital	Bajo
1	Control de Acceso	Definición de roles, privilegios y políticas de contraseñas	Área de sistemas	2/5/2025	5/1/2025	Finalizado	Documento aprobado por comité	Moderado
2	Dispositivos Móviles	Configuración y entrega de dispositivos a usuarios	Área de sistemas	2/23/2025	5/1/2025	Finalizado	Registro de entrega y configuración	Moderado
2	Seguridad Física y Ambiental	Evaluación de instalaciones, cableado, sistema eléctrico y mantenimiento de equipos	Área de sistemas, Autoridades ancestrales	2/24/2025	5/1/2025	Finalizado	Informe de evaluación	Moderado
2	Capacitación de personal	Sensibilización en políticas de seguridad	Autoridades ancestrales, Área de sistemas	2/25/2025	5/1/2025	Iniciado	Lista de asistencia, evidencias de capacitación	Moderado
3	Gestión de Copias de Seguridad	Implementación de procedimientos de backup y restauración	Área de sistemas	3/26/2025	5/1/2025	Iniciado	Procedimiento documentado	Moderado
3	Conexiones Remotas	Configuración segura de acceso remoto y portal cautivo	Área de sistemas	3/27/2025	5/1/2025	Iniciado	Reporte de configuración	Alta
3	Gestión de Incidentes	Definición de proceso de gestión de incidentes	Área de sistemas, Comité Técnico SI	3/28/2025	5/1/2025	Iniciado	Procedimiento y plantilla de reporte	Alta
4	Gestión de Activos	Procedimientos de entrega y devolución de activos	Área de sistemas, Jefes de área	4/2/2025	5/1/2025	Iniciado	Paz y salvo firmado	Moderado
4	Comunicaciones y Operaciones	Implementación de antivirus, antispam, monitoreo de eventos	Área de sistemas	4/15/2025	5/1/2025	No iniciado	Informes de configuración	Alta
4	Seguridad de Sistemas	Actualización de sistemas operativos, software y antivirus	Área de sistemas	31/4/2025	5/1/2025	Iniciado	Checklist de actualizaciones	Moderado
5	Control de Cumplimiento	Revisión legal y normativa de políticas de seguridad	Comisión jurídica, Autoridades ancestrales	4/1/2025	5/1/2025	No iniciado	Informe de cumplimiento	Alta
5	Capacitación Continua	Simulacros de incidentes y entrenamiento	Área de sistemas, Autoridades ancestrales	5/1/2025	5/1/2025	No iniciado	Registro de simulacros	Alta
6	Auditoría y Revisión	Evaluación de cumplimiento de políticas y controles	Comité Técnico SI, Auditoría interna	5/1/2025	5/1/2025	Iniciado	Informe final y plan de mejora	Alta
6	Ajustes y Mejora	Actualización de políticas y procedimientos	Comité Técnico SI	5/1/2025	5/1/2025	No iniciado	Políticas revisadas y aprobadas	Alta

PLAN DE TRATAMIENTO RIESGO CABILDO INDIGENA RESGUARDO JAMBALO							
AMENAZAS	ACTIVOS	Riesgo residual		Probabilidad	Evaluación	Medidas de mitigación de riesgo	Control
		cuantitativo	cualitativo				
Desconocimiento en seguridad de la información	Información		Moderado	Moderado	Moderado	Dar cumplimiento con los acuerdos de diligenciamiento de confidencialidad para todos los empleados	A.5.1.1 Políticas para la seguridad de la información A.5.1.2 Revisión de la política
Falta de capacidad para asignar funciones específicas en seguridad de la información	Talento Humano		Bajo	Bajo	Bajo	definir y asignar claramente las responsabilidades de seguridad de la información dentro de una organización	6.1.1 Asignación de responsabilidades para la segur. de la información.
Funcionarios con desconocimiento en temas de contratación de personal Cambios en las regulaciones y lineamientos del gobierno que puedan impactar las operaciones de la organización Insuficiente protección y privacidad de información personal	Información y Talento Humano		Moderado	Moderado	Moderado	Verificar la veracidad de los antecedentes de los funcionarios que esté acorde a las funciones u obligaciones laborales . Validar procedimiento de vinculación y retro laboral desde las áreas pertinentes y capacitar al personal en seguridad de la información para concientizar en buen manejo de seguridad	7.2.2 Concenciación, educación y capacitación en segur. de la información A.7.1.1 Selección A.7.1.2 Términos y condiciones del empleo A.7.2.3 Proceso disciplinario A.7.3.1 Responsabilidades en la terminación o cambio del empleo.
perdida de equipos	area administrativas		Bajo	Bajo	Bajo	Todos los empleados y usuarios de partes externas deberían devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	8.1.4 Devolución de activos.
Acceso no autorizado	administración de información en los equipos de computo bases de datos	Alto		Moderado	Alto	planes de control control de usuarios	9.4.3 Gestión de contraseñas de usuario.
Robo o hurto de información catalogada como sensible por falta de implementación de herramientas que aseguren el transporte de la información por la red	Información		Moderado	Alto	Alto	Implementación de controles criptográficos y gestión de claves criptográficas	A.10.1.1 Política sobre el uso de controles criptográficos
desastres naturales	daños por incendios de Información, Hardware software	Moderado		Moderado	Moderado	Respaldo de información copias de seguridad	11.1.4 Protección contra las amenazas externas y ambientales
Indisponibilidad de fluido eléctrico en el centro de datos y PCs	Información, Hardware software	Moderado		Moderado	Moderado	Realizar inspecciones periódicas de los equipos tecnológicos y de respaldo (servidores, UPS, planta eléctrica) para verificar su funcionamiento y ejecutar las correcciones necesarias	A.11.2.2 Servicios de suministro
estructuración del cableado red	red LAN	Moderado		Moderado	Moderado	adecuación de cableado	11.2.3 Seguridad del cableado
Falla en el Hardware	equipo de computo	Bajo		Bajo	Bajo	mantenimientos preventivos	11.2.4 Mantenimiento de los equipos.
Afectación en la disponibilidad del respaldo de la información. Insuficiencia de espacio o almacenamiento para el aseguramiento de la información. Pérdida o corrupción de los datos.	información		Moderado	Moderado	Moderado	política y procedimientos para la realización de backups a software, imágenes de los sistemas operativos, e información crítica Verificación de las copias de respaldo por medio de pruebas de restauración	12.3.1 Copias de seguridad de la información.
Fuga o pérdida de información generada por código malicioso. Divulgación no autorizada de información debido a acceso de terceros a través del uso de malware. Indisponibilidad de la información generada por virus informáticos.	Información, Hardware software		Alto	Moderado	Alto	Establecer e implementar políticas para la gestión de vulnerabilidades técnicas y para la restricción de instalación de software en sistemas operativos	A.12.6.2 Restricciones sobre la instalación de software

Evaluación de la Probabilidad

En la evaluar de la probabilidad de ocurrencia en el cabildo indígena resguardo de Jambalo de acuerdo a los riesgos establecidos

• Probabilidad Baja: Rara vez ocurre.
• Probabilidad Moderada: Ocurre ocasionalmente
• Probabilidad Alta: Ocurre con frecuencia.

Nivel de riesgo

Para evaluar el mapa de riesgo de la tabla plan de tratamiento de riesgo se hace un diagnóstico de la cantidad de evaluación al cumplimiento de los controles respectivos.

Nivel	Cantidad
Bajo	3
Moderado	6
Alto	3
Extremo	0

Mapa residual de riesgo

Para establecer el mapa de riesgo se mira la probabilidad respecto al impacto de riesgo que puede tener la organización frente métricas establecidas.

Mapa de Riesgo Residual				
PROBABILIDAD	IMPACTO			
	1 a 2- BAJO	3- MODERADO	4-ALTO	5- CATASTR OFICO
4 a 5 -ALTO				
3-MODERADO				
1 a 2 -BAJO				

ANEXO 3**MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA
INFRAESTRUCTURA TECNOLÓGICA EN EL CABILDO INDÍGENA RESGUARDO
DE JAMBALÓ.**

A continuación, se establecieron las políticas de seguridad para la infraestructura tecnológica en el cabildo indígena resguardo de Jambaló, se tomó como referencia la normatividad ISO 27001 y el marco de seguridad NIST, de igual forma se tuvo en cuenta la legislación autónoma del cabildo con el fin de garantizar la aplicabilidad de las políticas de seguridad

INTRODUCCION

En cumplimiento el cabildo indígenas resguardo de jambalo, establece políticas de seguridad de informacion, con el fin de garantizar la seguridad de todos sus activos por ende reconoce que la información es un activo indispensable para el cumplimiento de los objetivos misionales, siguiendo estrictamente los lineamientos de la política de calidad, por lo tanto, se preocupa por definir reglas que permitan evitar, trasladar o mitigar los posibles riesgos a los que se puede enfrentar dicha información durante el desarrollo de las actividades.

El presente manual describe los lineamientos y las políticas de seguridad de la información que integran el Sistema de Gestión de Seguridad de la Información (SGSI), basándose en las buenas prácticas de seguridad de la información ISO 27001

OBJETIVO

Establecer las políticas de seguridad de la información para el cabildo indígena resguardo de Jambaló, que se deben conocer y cumplir por todo el personal que labore en la organización sin importar el cargo de igual manera a terceros naturales o jurídicos que presten sus servicios o tenga alguna relación, con el fin de propender por la salvaguarda y preservación de la información, así como de los bienes y activos informáticos de la organización, garantizando la confidencialidad, integridad y disponibilidad de los mismos.

ALCANCE

Las políticas de Seguridad de la Información relacionadas en este manual, serán permeadas a todos los procesos estratégicos, de evaluación, misionales y de apoyo, estos lineamientos deberán ser socializados y cumplidos a cabalidad por todos los empleados administrativos, proveedores, contratistas y terceros, que tengan acceso a los sistemas de información e instalaciones físicas del cabildo indígena resguardo de jambaló.

TERMINOS Y DEFINICIONES

Activo: Bienes, derechos y otros recursos de los que dispone la Organización, pudiendo ser, por ejemplo, muebles, construcciones, equipos informáticos o derechos de cobro por servicios prestados o venta de bienes a clientes. También, se incluirían aquellos de los que se espera obtener un beneficio económico en el futuro

Política de Calidad: Documento de una extensión no mayor a una hoja que se integra en el manual de calidad y que demuestra el compromiso de la dirección de implantar un sistema de gestión de la calidad orientado a la atención del cliente y a la mejora continua.

Confidencialidad: Propiedad de la información que garantiza que la información es accesible sólo para aquellos autorizados a tener acceso" y es una de las piedras angulares de la seguridad de la información.

Integridad: Propiedad que busca mantener los datos libres de modificaciones no autorizadas. Salvaguarda la precisión y completitud de la información y sus métodos de proceso

Disponibilidad: Propiedad que asegura que los usuarios autorizados pueden acceder a la información cuando la necesitan

Mitigar: Se usa para referirse a que algo debe ser contrarrestado, moderado, suavizado, aplacar o suavizar la dureza de algo. En el caso de este manual se refiere a la manera de contrarrestar los riesgos.

Amenaza: Peligro latente, originado por un hecho o acontecimiento que aún no ha sucedido. Las amenazas pueden darse por fenómenos naturales como las inundaciones, o pueden ser causadas por el ser humano como los actos terroristas, incendios, etc.

Vulnerabilidad: Es una debilidad del sistema informático que puede ser utilizada para causar un daño.

Riesgos: Probabilidad de que una amenaza se materialice utilizando la vulnerabilidad existente de un activo, generando pérdidas o daños a la Organización.

Terceros: Todas las personas que prestan un servicio o se benefician de los servicios que ofrece la Organización (clientes, proveedores, contratistas, etc)

SGSI: Corresponde a las siglas de Sistema de Gestión de Seguridad de la Información.

Salvaguarda: En seguridad de la información hace referencia a defender o proteger los activos de la Organización.

Usuario: Persona que utiliza un dispositivo o un ordenador y realiza múltiples operaciones con distintos propósitos.

Autoridades ancestrales: Persona o conjunto de personas que tienen una responsabilidad general sobre toda la organización, responsable de dirigir la Organización en todas sus áreas.

Comité de Seguridad de la Información: Grupo de personas interdisciplinario que desarrollan actividades concernientes a la seguridad de la información de la Organización.

POLITICA GENERAL DE SEGURIDAD DE LA INFORMACION

El Cabildo Indígena Resguardo de Jambaló Cauca, entidad pública de carácter especial, sin ánimo de lucro, legalmente constituida por el ministerio del interior tiene una estructura política organizativa administrable de acuerdo a la ley de origen y derecho mayor, así como las normas contempladas en la ley 89 de 1980, los artículos 93, 246, 330 de la constitución política de Colombia, la declaración de las Naciones Unidas sobre los derechos de los pueblos indígenas y el convenio 169 de la OIT aprobada mediante la ley 21 de 1991.

En la constitución del 1991 ratifica los derechos de las organizaciones indígenas en la cual el decreto 1953 de 2014 garantiza la autonomía para administrar los recursos propios como régimen especial con el fin de poner en funcionamiento los territorios indígenas respecto de la administración de los sistemas propios de los pueblos indígenas hasta que el congreso expida la ley de que trata el artículo 329 de la Constitución Política.

El Cabildo Indígena Resguardo de Jambaló tiene una estructura política administrativa que a lo largo del tiempo ha permitido avanzar en los proyectos comunitarios orientados desde las asambleas con el propósito de avanzar en el desarrollo educativo, económico, salud y gobierno propio.

El cabildo indígena resguardo de Jambaló, es una empresa comunitaria. Está ubicado al nororiente del departamento del Cauca, a 80 kilómetros de la ciudad de Popayán. Limita por el norte con los municipios de Caloto y Toribío, por el oriente con el municipio de Páez, por el sur con el municipio de Silvia y por el occidente con los municipios de Caldono y Santander de Quilichao, en (Radioteca.net.) el cabildo indígena está conformado por las Autoridades

Tradicionales Nej Kwe'sx quienes por el mandato propio elegidos por la comunidad en la asamblea son las garantes y orientadores del cumplimiento de los derechos en defensa del territorio y de la autonomía política, jurídica o normativa, financiera y económica; fiscal, administrativa, cultural; de sus tradiciones espirituales, de su historia y de su ciencia como pueblos indígenas.

Se han establecido una serie de instrucciones para que toda el personal administrativos y terceros que interactúen de cualquier forma con la Organización, permitan con el cumplimiento de las mismas, garantizar la confidencialidad, integridad y disponibilidad de la información, siguiendo los ideales consignados en la política de calidad y de la mano del Sistema de gestión de Calidad.

Todos los usuarios internos o externos que hagan uso de los sistemas de información y telecomunicaciones de la Organización, tienen la responsabilidad y obligación de cumplir con las directrices y buenas prácticas de seguridad de la información estipuladas en el presente manual.

COMPROMISO DE LA DIRECCION

Las autoridades ancestrales consciente de la importancia que tiene para todas las organizaciones el Sistema de Seguridad de la Información, aprueba y se compromete a apoyar la estructuración e implementación de este Manual de Políticas de Seguridad de la Información, designando un equipo interdisciplinario competente (Comité de Seguridad de la Información) que realice la revisión, divulgación, actualización y generación de nuevas Políticas de Seguridad de la Información, acorde a los lineamientos de la estructura organizacional de la Organización .

De igual manera las autoridades ancestrales está comprometida a dar el reconocimiento al Comité técnico de Seguridad de la Información y asignar funciones, que le permitan supervisar el estricto cumplimiento de las políticas instauradas en el Manual de Seguridad y remitir los casos de incumplimiento de las mismas ante las autoridades ancestrales para la aplicación de las sanciones disciplinarias o legales a que tengan lugar, de acuerdo a la normatividad establecida por la organización indígena para todas las personas como (funcionarios administrativos, proveedores, contratistas y terceros).

POLITICAS DE SEGURIDAD DE LA INFORMACION

Política de estructura organizacional de seguridad de la información

Para el cabildo indígena resguardo de Jambaló es muy importante contar con una estructura organizacional de seguridad de la información definida, que permita la acertada toma de decisiones y que garantice la protección de los activos de información de la Organización.

La política de estructura organizacional de Seguridad de la Información se aplicará por la Organización definiendo los roles, responsabilidades y procedimientos lo cual compromiso del Comité técnico de Seguridad de la Información relacionados a continuación:

- Propender por el cumplimiento de las políticas y las buenas prácticas de seguridad de la información consignadas en el manual.
- Generar nuevas políticas y actualizar las políticas de seguridad de la información consignadas en el manual.
- Realizar el monitoreo constante de los incidentes de seguridad detectados o reportados por otras dependencias y realizar la gestión correspondiente para mitigar o trasladar el mismo.
- Identificar y ejecutar controles para los riesgos identificados.
- Programar y ejecutar auditorías internas al Sistema de Gestión de Seguridad de la Información, con el fin de verificar si las políticas, procedimientos y controles se encuentren alineadas con los objetivos planteados por la Organización para tal fin.

Comité técnico de seguridad:

Se establece un comité técnico de seguridad de la información en la infraestructura tecnológica del cabildo indígena resguardo de Jambaló que ayude a mitigar la seguridad de los activos y la información de la organización, además el comité tiene como objetivo buscar un equilibrio y asegurar una dirección y apoyo técnico gerencial al personal que labore, para buscar iniciativas propias sobre seguridad de la información, a través de un compromiso mutuo y el uso adecuado de los activos de la organización.

El comité de seguridad de la información está conformado de la siguiente manera:

- Apoyo técnico de la seguridad de la información
- Representante legal
- Autoridades ancestrales
- Responsable jurídica

Las autoridades ancestrales tendrán las siguientes responsabilidades:

El compromiso de las autoridades ancestrales y representante legal con el diseño de la propuesta metodológica para la implementación de un modelo para la gestión de la seguridad de la información en la infraestructura tecnológica en el cabildo indígena resguardo de Jambaló, muestra el compromiso como organización indígena para el desarrollo y el fortalecimiento de las buenas prácticas de las políticas de seguridad contenidas en este documento.

Compromisos:

- Aprobar las Políticas de Seguridad de la Información.

- Aprobar los roles y responsabilidades de los funcionarios relacionados con la seguridad de la información.
- Asignar recursos, infraestructura física y personal necesario para la gestión de la seguridad de la información en la Organización.
- Definir los lineamientos para el contacto con las autoridades en caso que se requiera alguna intervención por parte de los mismos.

Política para uso de dispositivos móviles

La Organización define las directrices para el uso responsable y manipulación de los dispositivos móviles institucionales (teléfonos convencionales, teléfonos inteligentes y tablets) asignados a las personas que hagan uso de estos activos o servicios de la organización.

- Apoyo técnico de la seguridad de la información deberá entregar los dispositivos móviles debidamente instalados y configurados con los requerimientos de seguridad y las aplicaciones necesarias para el uso adecuado de los mismos por parte de los usuarios.
- El área de sistema deberá implementar un método para realizar las copias de seguridad a la información procesada y contenida en los dispositivos móviles organización.
- El área de sistema deberá instalar y configurar un software antivirus en cada uno de los dispositivos móviles organización.
- Los usuarios no podrán retirar los dispositivos móviles de las instalaciones de la Organización sin autorización y sin la debida justificación. En caso de que se

autorice la salida de estos dispositivos, el usuario deberá evitar el uso de los mismos en lugares donde sean expuestos a hurto, pérdida o daños irreparables a los equipos.

- Los usuarios solo podrán conectar los dispositivos móviles a las redes inalámbricas de la Organización. Los servicios de Bluetooth, Ubicación o Infrarrojos deberán permanecer deshabilitados.
- Los usuarios deben evitar conectar los dispositivos móviles a través de cables USB a equipos de cómputo que no pertenezcan a la Organización.
- Los usuarios deben evitar conectar los dispositivos móviles con adaptadores de voltaje diferentes a los asignados con el equipo.
- Los usuarios no deben modificar las configuraciones de seguridad de los dispositivos móviles institucionales asignados.
- Los usuarios no deben instalar aplicaciones o programas diferentes a las que se encuentren en los dispositivos móviles institucionales asignados.
- Los usuarios no podrán eliminar ninguna aplicación o programa que se encuentre configurado en los dispositivos móviles institucionales asignados.
- Los usuarios deberán activar y aplicar las actualizaciones que soliciten los dispositivos móviles institucionales cada que se requiera.
- Los usuarios no deben almacenar ningún tipo de información personal en los dispositivos móviles institucionales asignados.
- La información contenida en los dispositivos móviles institucionales (contactos, calendarios, tareas, entre otras), es propiedad exclusiva de la Organización como

titular de la misma. Por tanto, el usuario no podrá eliminar, modificar, divulgar o difundir dicha información sin autorización del comité de seguridad.

- Los usuarios no deben realizar llamadas internacionales desde los dispositivos móviles institucionales.
- Los usuarios deberán reportar cualquier anomalía que presenten los dispositivos móviles institucionales a su jefe inmediato y no podrán realizar ningún tipo de reparaciones técnicas al mismo.

Política para uso de Conexiones Remotas

La Organización establece las directrices para la realización de las conexiones remotas a la plataforma, redes de transmisión de datos, los recursos tecnológicos y los sistemas de información de la Organización.

- En área sistemas garantizará que los métodos y procedimientos que se realicen, tengan los niveles óptimos de seguridad durante la ejecución de las actividades remotas.
- En área sistemas permitirá el acceso de los usuarios autorizados a establecer conexión remota a la plataforma, redes de transmisión de datos, los recursos tecnológicos y los sistemas de información de la Organización.
- Los usuarios autorizados a realizar conexión remota deben acatar las normas y directrices establecidas para tal fin, desde los equipos de cómputo de la Organización y en los tiempos establecidos para ello.

Política de seguridad para los recursos humanos

El cabildo indigena resguardo de jambalo realiza acciones pertinentes para garantizar que la política de confidencialidad y buen uso de los recursos tecnológicos sean incluidos en los contratos o cualquier formato de vinculación laboral de funcionarios administrativos, contratistas y terceros, que tengan acceso a las instalaciones físicas y sistemas de información de la Organización.

Para conseguir los objetivos planteados es necesario capacitar y sensibilizar durante la inducción a los funcionarios y demás colaboradores, sobre las políticas de seguridad de la información, para lograr que estos adopten responsabilidades en relación con las políticas mencionadas y apliquen las directrices consignadas en estos documentos, en cada una de sus actividades laborales dentro y fuera de la Organización.

Es importante difundir periódicamente a través de cualquier medio de comunicación masiva, los cambios o actualizaciones que se apliquen a la política de confidencialidad y buen uso de los recursos tecnológicos y a todas las políticas de seguridad de la información aprobados por parte de las autoridades ancestrales. Lo anterior con el fin de generar una cultura de seguridad de la información, que permita a los actores principales de estas políticas, reducir los posibles riesgos a los que se expone la Organización por el uso inadecuado de los equipos dispuestos para el tratamiento de la información.

- Las autoridades ancestrales o jefe administrativo o quien realice las funciones de contratación, debe asegurar antes de la vinculación que el personal a contratar debe conocer las políticas de seguridad y los controles pertinentes.

- Las autoridades ancestrales o jefe administrativo o quien realice las funciones de contratación debe verificar los antecedentes del personal aspirante
- Las autoridades ancestrales o jefe administrativo o quien realice las funciones de contratación debe asegurar que el personal conozca sus responsabilidad y funciones a su rol
- Al presentarse un cambio o retiro del personal contratado las autoridades ancestrales o jefe administrativo debe hacer una nueva selección de aspirantes para el cargo pertinente.
- Al finalizar el contrato laboral con la organización del personal saliente debe firmar un acuerdo de confidencialidad.

Política de gestión de activos de información

El cabildo indigena resguardo de jambaló es propietaria de los activos de información físicos (equipos de cómputo tipo servidor, equipos de cómputo tipo estaciones de trabajo, equipos de cómputo tipo portátiles, impresoras, teléfonos, dispositivos de redes, entre otros), los servicios (internet, correo electrónico, aplicaciones), la información (generada, procesada, almacenada y transmitida) y los avances tecnológicos e intelectuales desarrollados por el personal de la Organización , derivados del cumplimiento de las funciones y tareas asignadas.

La Organización implementa las directrices relacionadas a continuación, con el fin de garantizar la protección y el buen uso de los activos de información por parte de los usuarios responsables de los mismos.

- Las autoridades ancestrales podrán supervisar y utilizar la información procesada por el empleado en los equipos de cómputo de la Organización en el momento que se requiera.
- El área de sistema deberá poseer disponible y actualizado el inventario de los activos de información con los que cuenta la Organización.
- El área de sistema deberá entregar los activos informáticos con la configuración adecuada, para que los usuarios realicen las tareas asignadas, propendiendo por la seguridad de la información y haciendo un uso adecuado de ellos.
- El área de sistema deberá garantizar que los activos de información estén protegidos por reguladores de voltajes y sus instalaciones eléctricas.
- El área de sistema debe recibir los activos informáticos de los usuarios que se retiran o cambian de labores, realizar las copias de seguridad pertinentes y reasignar dichos activos de acuerdo a las necesidades requeridas o planteadas por el usuario.
- El área de sistema deberá autorizar la instalación, actualización o eliminación de cualquier tipo de software o hardware configurado en los activos de información.
- El área de sistema realizara el control y la verificación de cumplimiento de licenciamiento del respectivo software y aplicaciones instaladas.

- El área de sistema deberá garantizar que todos los recursos informáticos estén protegidos mediante herramientas y software de seguridad como antivirus, antispam y antispymware.
- El área de sistema podrá realizar el monitoreo permanente de tiempos de navegación y páginas visitadas por parte de los funcionarios, contratistas y terceros.
- El área de sistema podrá bloquear o restringir el acceso a paginas o sitios públicos en Internet, cuyo contenido atente contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica de la Organización.
- Cada usuario es responsable del cuidado y uso adecuado de los recursos informáticos que se le asignen para el desarrollo normal de sus funciones, velando por la integridad, confidencialidad, disponibilidad, y auditabilidad de la información.
- Los usuarios de activos de información no podrán usar los elementos de cómputo asignados para realizar actividades personales distintas a las contratadas.

Los usuarios de activos de información no podrán comer, beber o fumar en los puestos de trabajo, centros de cómputo o instalaciones con equipos tecnológicos.
- Los usuarios no podrán destapar, modificar, reubicar o sustraer equipos de cómputo, software, información o periféricos de las instalaciones de la Organización sin la debida autorización.
- Los usuarios no podrán utilizar los activos informáticos de la Organización para acceder, descargar, imprimir, almacenar, transmitir o distribuir material pornográfico.

- Los usuarios no podrán desinstalar o desactivar el software de protección de antivirus, antispam o antispymware instalado y configurado en los recursos informáticos de la Organización.
- Los usuarios podrán hacer uso de los diferentes medios de almacenamiento removibles (memorias USB, CD, discos duros externos, etc.) para el procesamiento de la información de la Organización, en la medida que cumplan las políticas de seguridad establecidas para prevenir la propagación de virus o código malicioso.
- El envío masivo de mensajes publicitarios organizativo deberá contar con la aprobación del área de comunicaciones.
- La Organización podrá supervisar y utilizar la información procesada por el usuario en el correo corporativo en el momento que sea requerido por una orden judicial o por procesos internos de la organización. En cualquiera de los casos, la Organización notificara al usuario sobre el proceso a realizar en el momento de su ejecución.
- Los usuarios no podrán utilizar la dirección de correo organizativo como punto de contacto en comunidades interactivas de contacto social, como Facebook, Instagram, entre otras, o cualquier otro sitio que no tenga que ver con las actividades laborales.
- Los usuarios no podrán utilizar la dirección de correo organizativo para enviar cadenas de correo, mensajes con contenido religioso, político, racista, sexista, pornográfico, que vayan en contra de la moral, las leyes, y las buenas costumbres, publicitario no corporativo o cualquier tipo de mensajes que atenten contra la

dignidad, la productividad de las personas o el normal funcionamiento del servicio de correo electrónico en la Organización.

- Los usuarios deben bloquear la pantalla de su equipo de cómputo o cerrar sesión cuando dejen su puesto de trabajo.
- Los usuarios deben verificar en las impresoras, escáneres, fotocopadoras y máquinas de fax, no haber dejado al alcance de personas no autorizadas, documentos con información confidencial que al ser divulgada ponga en riesgo la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica de la Organización.
- Los usuarios no podrán reutilizar el papel impreso que contenga información confidencial que al ser divulgada ponga en riesgo la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica de la Organización.
- El usuario no podrá configurar impresoras remotas, red o locales diferentes a las asignadas para su uso en las instalaciones de la Organización.
- deberá ubicar o reubicar las impresoras en lugares en los cuales, la información impresa no quede expuesta al acceso sin control de invitados.
- Los usuarios deberán constatar que en su puesto de trabajo no queden expuestos al alcance de personas no autorizadas, unidades de almacenamiento extraíble (memorias USB, cd, discos duros extraíbles) con información sensible y confidencial para la Organización.

Política de Control de Acceso a la Información

El cabildo indígena resguardo de jambalo define las reglas para garantizar la creación, modificación, bloqueo o eliminación de las cuentas de usuario, que permiten el acceso lógico a los recursos tecnológicos y los sistemas de información de la Organización.

- En cada área de trabajo el personal que labora es responsable por pérdida de su información
 - Los usuarios son responsables del uso de claves y contraseñas en los equipos de computo
 - Las autoridades ancestrales deben monitorear la información está suministrando el equipo de comunicaciones en sitio WEB oficial del Cabildo Indígena.
 - Los archivos y carpetas almacenados en la red son propiedad del Cabildo Indígena.
 - Cada funcionario debe estar identificado con su credencial.
 - Se establecen políticas de manejo de contraseñas seguras, autenticación multifactorial y monitoreo de actividades de acceso para detectar comportamientos anómalos
 - El área de sistema deberá realizar la creación de las cuentas de acceso de los funcionarios a los sistemas de información de la Organización, previa solicitud.
- El área de sistema deberá establecer privilegios y accesos a los recursos tecnológicos y los sistemas de información de la Organización, a los usuarios de

dichos activos, de acuerdo a las funciones y requerimientos de información pertinentes a cada cargo o rol.

- El área de sistema deberá definir para las contraseñas de las cuentas de acceso, los lineamientos de longitud, complejidad, cambio periódico, bloqueo por número de intentos fallidos, control histórico y cambio de contraseñas, que serán aplicadas por los funcionarios a los sistemas de información de la Organización.
- El área de sistema deberá eliminar, bloquear o deshabilitar las cuentas de acceso de aquellos funcionarios, que finalizado el periodo laboral sean sancionados o no tengan ningún vínculo laboral con la Organización.
- Los usuarios deberán cambiar la contraseña de acceso a los recursos tecnológicos y sistemas de información de la Organización cuando ingresen por primera vez a la misma, teniendo en cuenta los lineamientos dispuestos por el proceso de tecnología para tal fin.
- Los usuarios no podrán ceder su cuenta de usuario (login) y contraseña (password) a ningún funcionario, para acceder a los recursos tecnológicos o sistemas de información de la Organización.
- Los empleados no podrán suministrar ni delegar las cuentas de usuario en periodo de ausencia, calamidad o vacaciones.
- Los usuarios propietarios de las cuentas de acceso generadas por el proceso de tecnología, son los únicos responsables de las acciones que se realicen logueados (login y password) con dichas cuentas en los sistemas de información.

Política de Gestión de Copias de Seguridad de la Información

El cabildo resguardo de jambalo define los lineamientos que permitan garantizar que toda la información almacenada en los diferentes componentes de los sistemas de información de la institución, se encuentren debidamente consignados en un lugar seguro permitiendo su respaldo en caso de requerirlo y mitigando el riesgo de pérdida de la información.

- El área de sistema deberá definir el procedimiento que detalle la periodicidad, medio de almacenamiento y permisos que deben acatar los funcionarios del cabildo al realizar la copia de seguridad de la información procesada, de tal manera que garanticen la protección, integridad y disponibilidad de la misma.
- El área de sistema deberá establecer un plan de restauración parcial y total de la información procesada y salva guardada en los diferentes medios adoptados por la institución para tal fin.
- El área de sistema deberá garantizar el cumplimiento de las condiciones básicas (sistema eléctrico, seguridad en el acceso, sistema eléctrico de respaldo, extintores y alarmas) para el funcionamiento adecuado de los servidores de almacenamiento de las copias de seguridad de la información organizativa.
- El área de sistema deberá definir conjuntamente con los departamentos de archivo y calidad, la rotulación y los periodos de retención y eliminación de las copias de seguridad de la información procesada y almacenada en los servidores de la Organización.
- Los usuarios son los responsables directos de la información procesada y almacenada en los equipos de cómputo de la Organización, por tanto, es su responsabilidad proteger la confidencialidad e integridad de la misma.

- Los usuarios deberán salvaguardar la información que procesan en cada uno de sus equipos de cómputo, siguiendo las instrucciones sobre el lugar de destino, periodicidad y procedimiento a realizar, designadas por el proceso de Tecnología para tal fin.
- Los usuarios no deberán utilizar los medios de almacenamiento extraíbles (CD, USB, discos duros externos, celulares, tablets) para salvaguardar la información procesada en sus equipos de cómputo.
- Los usuarios no podrán almacenar la información procesada en medios o destinos diferentes (escritorio, archivos de programa, carpeta Windows, entre otros) a los relacionados por el área de sistema para llevar a cabo tal fin.
- Los usuarios deberán subir a su cuenta organizativa de Google drive, la carpeta que contiene la copia de seguridad de su información procesada, la cual deberá estar identificada con nombre, una vez finalice su contrato laboral con la organización.
- Los usuarios no podrán almacenar información personal en la carpeta de destino de la copia de seguridad organizacional, puesto que este tipo de información no se considera prioritaria para la Organización.
- Los usuarios no tendrán acceso a los servidores de almacenamiento de la copia de seguridad de la información institucional. En caso que se requiera realizar el respaldo de información identificada como perdida o dañada, se deberá presentar la solicitud al proceso de Tecnología quien realizara el procedimiento.

Política de Acceso a Redes Inalámbricas

El cabildo resguardo de jambaló define los lineamientos para garantizar que todos los funcionarios, proveedores y terceros que requieran acceder a la red inalámbrica propiedad de la organización, puedan realizar sus actividades con eficiencia y cumpliendo a cabalidad con los directrices estipuladas para garantizar la confidencialidad, integridad y disponibilidad de la información de la Organización.

- El área de sistema deberá configurar los equipos de telecomunicaciones que conforman la red inalámbrica, de tal manera que sea visible para los dispositivos electrónicos de los funcionarios y terceros y garantizar que dicha conexión es segura.
- El área de sistema debe asegurar que las redes inalámbricas de la Organización, cuenten con los requisitos o controles para que los usuarios que se conecten a ella, se autenticuen y validen, permitiendo evitar accesos no autorizados a la misma.
- El área de sistema debe verificar constantemente las configuraciones de los controles de acceso de los usuarios antiguos y nuevos a la red inalámbrica de la Organización, con el fin de verificar que los usuarios tengan acceso únicamente a los recursos permitidos para el desarrollo de sus actividades.
- El área de sistema deberá estructurar un portal cautivo, que permita la administración de las cuentas de acceso requeridas por los usuarios (funcionarios y terceros) que deseen conectarse a las redes inalámbricas de la Organización.
- Los usuarios que requieran hacer uso de las redes inalámbricas de la Organización, deberán dirigirse a las oficinas del área de sistemas con la

identificación respectiva, para realizar la solicitud de una cuenta de acceso al portal.

Claves o contraseñas.

Las contraseñas deben tener al menos cuatro caracteres entre minúsculas y mayúsculas, números

- Las contraseñas deben poseer un grado de complejidad.
- Se debe cambiarlas contraseñas si presentar anomalías extrañas en tus dispositivos
- Las contraseñas no deben estar visibles al momento de ingresar al computador
- No revelar su contraseña a personas externas

Políticas de Seguridad Físicas y Ambientales

Prevenir el acceso físico no autorizado, por pérdida de daños de la información en la infraestructura tecnológica en el cabildo indígena resguardo de Jambaló y prevenir la alteración por pérdida o daños de los activos a continuación se documentan las políticas de seguridad física y ambiental de la organización.

- Solo en personal de sistemas es el encargado de realizar el mantenimiento de los equipos de computo
- Los equipos ingresados externos por el personal que labora debe ser registrado la organización no se hace responsable por perdida
- Los empleados no deben tener información confidencial en sus unidades de almacenamiento

- Debe existir planos el cableado estructurado
- El mantenimiento de equipos por parte de las personas encargadas debe estar programadas
- Se debe tener actualizada la información de los activos
- Todo el personal debe apagar los equipos al momento de finalizar la jornada
- Todo el personal debe suspender los equipos al momento de salir de la oficina en la hora de almuerzo para evitar pérdida de información.

Gestión de Incidentes

Se establece un proceso formal de gestión de incidentes para detectar, reportar, investigar y responder a incidentes de seguridad de manera rápida y efectiva.

- Se realizan simulacros periódicos de incidentes para entrenar al personal y mejorar la capacidad de respuesta ante situaciones de emergencia.

Política de cumplimiento

Todo el personal que esté vinculado laboralmente en el cabildo debe cumplir con todas las políticas de seguridad y evitar violaciones legales y queda sujeto al cumplimiento obligatorio de las normas expuestas, evitar sanciones o llamados de atención hasta la suspensión o retiro del cargo si es necesario.

CONTROLES DE SEGURIDAD

Los controles que a continuación se mencionan fueron elaborados con base referencial al ANEXO A de la normatividad colombiana NTC-ISO/IEC 27001.

Objetivo

Brindar instrucciones del buen uso de los activos de la información y recomendaciones de las políticas de seguridad con el fin de proteger la integridad de la información.

Política de Seguridad de la Información:

- Las políticas de seguridad elaboradas para la infraestructura tecnológica en el cabildo indígena resguardo de Jambaló será dada a conocer al momento de la vinculación con la organización de igual forma cada empleado está en el ejercicio obligatorio de cumplir, a su vez sirve como orientación o instrucciones que brindan apoyo respecto a la seguridad de la información de acuerdo con los requisitos y leyes pertinentes.
- El área de sistemas o auxiliares técnicos están en la obligación de incorporar estas reglas de seguridad y de la revisión periódicamente al tiempo estipulado por las autoridades ancestrales de dos veces al año y revisar el cumplimiento.
- Capacitar al personal sobre la importancia y el cumplimiento de la política de seguridad de la información.

- Las autoridades ancestrales validarán el cumplimiento y revisión de las políticas de seguridad elaboradas.

Control para la Organización de la Seguridad de la Información:

- Desde las autoridades ancestrales y equipo técnico deben mantener y gestionar la información procesada dentro de la organización y orientar a todo el personal.
- El departamento jurídico de la organización en conjunto con las autoridades ancestrales debe redactar un documento de confidencialidad en el que obliga al empleado de no divulgar información ni activos de la organización, este documento debe ser firmado antes de la contratación y archivado junto con la hoja de vida
- Las autoridades ancestrales deben validar la información suministrada por el empleado antes de la contratación, revisar sus antecedentes y explicar los deberes y responsabilidades de seguridad.
- El usuario de la organización debe ser informado sobre el tratamiento de datos.
- Las funciones y responsabilidades deben comunicarse al personal que labora después de la contratación para el desarrollo de sus actividades

Gestión de activos de Información:

- Identificar los activos y definir las responsabilidades de la protección adecuada de la información de los registros de inventarios.
- Realizar inventarios periódicos de los activos de información y tecnológicos.
- Etiquetar y clasificar los activos de acuerdo con su importancia y sensibilidad.

- Establecer procedimientos para el manejo seguro de activos, incluyendo disposición adecuada de equipos obsoletos.
- El jefe de cada área o coordinadores y empleado con activos asignados, deberá dar información del equipo asignado y el empalme de la información generada en su periodo de contratación.
- El personal que sea retirado o removido del cargo deberá devolver en perfecto estado los equipos tecnológicos al encargado de sistemas.
- El empleado deberá firmar un documento de paz y salvo generado desde las autoridades ancestrales para la desvinculación con la organización.

Control de Acceso:

- Establecer medidas preventivas para limitar el control de acceso no autorizado de la información como, control de acceso a redes, servicios y asignación de privilegios especiales.
- Establecer controles de acceso físico a las instalaciones donde se encuentran los activos de información y tecnológicos.
- Implementar autenticación de dos factores para acceder a sistemas y datos sensibles.
- Asignar roles y privilegios de acceso de acuerdo con las responsabilidades de cada usuario.
- Las autoridades ancestrales deben brindar herramientas necesarias o métodos que permitan establecer la política de control.

- Es responsabilidad del área de sistemas exigir a todo el personal del cabildo indígena que trabaje con la organización el cumplimiento de las buenas prácticas de seguridad, el uso de contraseñas y cumplir con las políticas de seguridad.

Controles de Gestión de Comunicaciones y Operaciones

- Asegurar la protección de la información manteniendo la disponibilidad, la integridad y protección de la infraestructura tecnológica de incidentes
- Las autoridades ancestrales deben adelantar las gestiones de adquisición de un sistema de detección de intrusos que permita mitigar los riesgos de seguridad
- El área de sistemas debe garantizar que la información está protegida por software maliciosos
- Implementar herramientas de monitoreo de eventos y registros de actividad para detectar posibles amenazas o incidentes de seguridad.
- El área de sistemas debe implementar controles idóneos para la protección de la información como instalación y actualización de los antivirus
- Revisar regularmente los registros de eventos para identificar patrones o comportamientos anómalos.
- El área de sistemas debe establecer copias de seguridad de la información

Seguridad de Equipos y Sistemas:

- Garantizar la protección de seguridad de la información como parte fundamental en el ciclo de vida de los sistemas de información.
- Las autoridades ancestrales en ejercicio de sus funciones deben suministrar los recursos para la seguridad de la información para que desde el área de sistemas verifiquen los procedimientos y políticas de seguridad de los sistemas.
- El área de sistemas debe controlar la instalación de programas por los funcionarios solo si sea autorizado
- Mantener actualizados los sistemas operativos, aplicaciones y antivirus en todos los equipos.
- Realizar copias de seguridad periódicas de la información crítica y almacenarlas en un lugar seguro.

Gestión de incidentes de seguridad:

- Garantizar un enfoque consistente y eficaz para la gestión de incidentes de seguridad de la información de las responsabilidades, procedimientos y tomar acciones correctivas oportunamente.
- Establecer un proceso de gestión de incidentes para responder rápidamente a incidentes de seguridad, investigar sus causas y tomar medidas correctivas.
- Notificar a las partes afectadas y a las autoridades competentes en caso de incidentes graves que afecten la confidencialidad o integridad de los datos.

- Proporcionar capacitación continua sobre seguridad de la información y concientización sobre la importancia del uso seguro de activos y datos.
- Realizar simulacros de incidentes de seguridad para preparar al personal para situaciones reales.

Control de Cumplimiento.

- Evitar el incumplimiento de las obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información de la infraestructura del cabildo indígena resguardo de Jambaló de acuerdo con las políticas y procedimientos organizacionales.
- Las autoridades ancestrales en sus usos y facultades tienen el deber de hacer cumplir a todo el personal del cabildo indígena las responsabilidades y procedimientos de las políticas y controles pertinentes
- La comisión jurídica debe de identificar las responsabilidades y procedimientos de los requisitos estatutarios y de autonomía propia aplicable para verificar el cumplimiento de las normas.
- El comité técnico de seguridad es el responsable de monitorear que los activos sean utilizados correctamente.

Nota

Los controles mencionados son de estricto cumplimiento para todo el personal que tenga vínculo directa o indirectamente con el cabildo indígena y evitar violaciones legales y queda sujeto al cumplimiento obligatorio a las normas expuestas, evitar sanciones o llamados de atención hasta la suspensión o retiro del cargo si es necesario.

**CERTIFICADO APROBACION MANUAL DE POLITICAS DE SEGURIDAD DE
LA INFORMACION.**



BAT UKWE CXHABTE KHA'BUWESX SA'T TAMA KIWE
CABILDO INDIGENA RESGUARDO JAMBALO
CAUCA COLOMBIA.

Car. 5 No 5-68 Tel: - 3226200322

NIT 817003136 — 0

E-mail - cabildojambalo@gmail.com

N°001

LOS NEJ WESX "AUTORIDADES ANCESTRALES" DEL RESGUARDO INDIGENA DE JAMBALO - CAUCA, EN USO DE LAS FACULTADES LEGALES QUE LE CONFIERE LA LEY 89 DE 1890, LA CONSTITUCION POLITICA DE COLOMBIA EN SUS ARTICULOS 246 Y 330 RATIFICADOS EN EL CONVENIO 169 DE LA OIT RATIFICADO EN LA LEY 21 DEL 91 Y DESDE LA LEY DE ORIGEN Y LOS MANDATOS COMUNITARIOS.

aprobación:

A: **JERSON RONALDO MARTINEZ TROCHEZ** Identificado con Cedula de Ciudadania N° **1.061.504.283** expedida en Jambalo Cauca, Pertenece a este Resguardo indígena conserva su identidad cultural como Nasa, cuenta con su residencia en la vereda Nueva Colonia, Resguardo - Municipio de Jambalo. Por lo tanto se encuentra inscrita en el censo poblacional que la Autoridad ancestrales lleva en su despacho. El cabildo indígena resguardo de jambaló en nombre de las Autoridades ancestrales y el encargado de sistemas aprueban **MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA INFRAESTRUCTURA TECNOLÓGICA EN EL CABILDO INDIGENA RESGUARDO DE JAMBALÓ.**

Para validez se firma en la oficina de Las Autoridades Ancestrales a los 20 días del mes de enero-2025.

Imax C. Ortiz Conda
Iris Cenoviet Ortiz Conda
Nej We'sx- Autoridad Ancestral

Iris Noralba Yatacue Trochez
Iris Noralba Yatacue Trochez
Nej We'sx- Autoridad Ancestral

Rosaura Zapata
Rosaura Zapata
Nej We'sx- Autoridad Ancestral

Wilmar Ariel Padua Conda
Wilmar Ariel Padua Conda
Nej We'sx- Autoridad Ancestral

Wilson Alfredo Cualla Ipiá
Wilson Alfredo Cualla Ipiá
Nej We'sx- Autoridad Ancestral

Nancy Betancur Quiguañas
Nancy Betancur Quiguañas
Tache Thegnas

Filmon Medina Cueta
Filmon Medina Cueta
Coord. Plan de Vida - P. G

ANEXO 5. AVAL



BAT UKWE CXHABTE KHA'BUWESX SA'T TAMA KIWE
CABILDO INDIGENA RESGUARDO JAMBALO
CAUCA COLOMBIA.

Car. 5 No 5-68 Tel: - 3226200322

NIT 817003136 — 0

E-mail - cabildojambalo@gmail.com

Nº002

LOS NEJ WESX "AUTORIDADES ANCESTRALES" DEL RESGUARDO INDIGENA DE JAMBALO - CAUCA, EN USO DE LAS FACULTADES LEGALES QUE LE CONFIERE LA LEY 89 DE 1890, LA CONSTITUCIÓN POLITICA DE COLOMBIA EN SUS ARTICULOS 246 Y 330 RATIFICADOS EN EL CONVENIO 169 DE LA OIT RATIFICADO EN LA LEY 21 DEL 91 Y DESDE LA LEY DE ORIGEN Y LOS MANDATOS COMUNITARIOS.

CERTIFICAMOS:

A: **JERSON RONALDO MARTINEZ TROCHEZ** Identificado con Cedula de Ciudadanía Nº **1.061.504.283** expedida en Jambalo Cauca, Pertenece a este Resguardo indígena conserva su identidad cultural como Nasa, cuenta con su residencia en la vereda Nueva Colonia, Resguardo - Municipio de Jambalo. Por lo tanto se encuentra inscrita en el censo poblacional que la Autoridad ancestrales lleva en su despacho. El cabildo indígena resguardo de jambaló en nombre de las Autoridades y la Representante legal Thace Thena. **Ha revisado, evaluado y aprobado** el proyecto de grado

Titulado diseño de una propuesta metodológica para la gestión de la seguridad de la información en la infraestructura tecnológica en el cabildo indígena resguardo de jambaló. Para optar el título de Ingeniero de Sistemas en la **CORPORACION UNIVERSITARIA COMFACAUCA UNICOMFACAUCA**

Este proyecto tuvo como objetivo a portar al proceso organizativo como plan de vida Proyecto Global para garantizar la protección, integridad, confidencialidad y disponibilidad de la información, alineándose con los principios de, tierra, cultura.

Se hace constar que el presente documento refleja el compromiso del estudiante, la comunidad y las Autoridades para la correcta implementación y seguimiento de las políticas establecidas en el Sistema de Gestión de Seguridad de la Información SGSI.

Para validez se firma en la oficina de Las Autoridades Ancestrales a los 1 días del mes de mayo-2025.

Irma C. Ortiz Conda
Irma Cenoviet Ortiz Conda
Nej We'sx- Autoridad Ancestral

Iris Noralba Yatacue Trochez
Iris Noralba Yatacue Trochez
Nej We'sx- Autoridad Ancestral

Rosaura Zapata
Rosaura Zapata
Nej We'sx- Autoridad Ancestral

Wilmar Ariel Pardo Conda
Wilmar Ariel Pardo Conda
Nej We'sx- Autoridad Ancestral

Wilson Alfredo Cuesta Ipiá
Wilson Alfredo Cuesta Ipiá
Nej We'sx- Autoridad Ancestral

Nancy Betancur Quiguañas
Nancy Betancur Quiguañas
Taçe Thegnas

Filmon Medina Cuetia
Filmon Medina Cuetia
Coord. Plan de Vida - P. G

