Auditoria De Seguridad Informática Cabildo Indígena De Corinto alineadas al COBIT 5 e ISO 27001

Billy Kennedy Atillo Campo y Nicolás Santiago Iles Rodríguez

Notas de Autor

Billy Kennedy Atillo Campo y Nicolás Santiago Iles Rodríguez, Ingeniería En Sistemas,

Fundación Universitaria de Popayán (Sede Norte)

Esta tesis ha sido financiada por los autores del mismo

Nota de Aceptación

Aprobado por el Comité de Grado en cumplimiento de los requisitos exigidos por la Fundación Universitaria de Popayán para optar al título de Ingeniero de Sistemas

---

Juan Pablo Arango

Subdirector

Programa Ingeniería de Sistemas

Fundación Universitaria de Popayán

Sede Norte del Cauca

José Fernando Mera

Director Trabajo de Grado

Firma Jurado 1

Firma Jurado 2

Dedicatoria

La presente tesis está dedicada a Dios, a los espíritus de la madre naturaleza, ya que gracias ellos hemos podido concluir la carrera satisfactoriamente.

A nuestros padres, que con sus esfuerzos y apoyos incondicionales siempre estuvieron a nuestro lado dándonos consejos para hacernos unas personas de bien.

A nuestros hermanos, primos, nuestras familias (Abuelos, Tíos), amigos y en su momento nuestras parejas, que estuvieron dándonos ánimos para terminar nuestra carrera, ese apoyo emocional y mental sin condiciones para así ser unos grandes profesionales.

Por ultimo a nuestros Tutores, Profesores, Directores de la FUNDACION UNIVERSITARIA DE POPAYAN (FUP) quienes ayudaron a nuestra formación profesional, por su paciencia, confianza y la fé que tenían e nosotros para poder culminar. A nuestro Director inolvidable ALEJANDRO OSPINA que hoy desde el cielo nos guía, nos orienta para asi terminar satisfactoriamente esta carrera de Ingeniería de Sistemas, quien lucho y por destino de Dios no pudo estar presente en la sustentación de tesis y nuestro grado, se lo dedicamos a él este gran logro.

Agradecimientos

Agradecerle primeramente a Dios, a nuestros Padres, Docentes, Directores, Compañeros de Estudio (FUNDACION UNIVERSITARIA DE POPAYAN), a la Universidad, familiares y Amigos quienes contribuyeron a nuestra formación profesional para así culminar nuestra carrera de Ingeniería de Sistemas a cada uno de ellos por apoyarnos, orientarnos es gracias a ellos que estamos logrando este gran objetivo.

A todos mil y mil gracias.

Tabla de Contenido

Tabla de Ilustraciones

Lista de Tablas

Glosario

Acciones legales[1]: “La acción jurisdiccional es el derecho de acceso a los juzgados y tribunales solicitando que ejerzan la potestad de juzgar y hacer ejecutar lo juzgado.

Activo de Información[2]: “Es todo aquello que las entidades consideran importante o de alta validez para la misma ya que puede contener importante información.

Tipos de Acceso[3]: “Se definen valores de privilegios, de esta forma hay usuarios que pueden administrar las contraseñas del sistema. Otros usuarios pueden administrar la aplicación de respaldo. Cada uno de estos privilegios puede ser asignado a ciertos usuarios.

Criptografía: Técnicas de cifrado o codificado destinadas a alterar las representaciones lingüísticas de ciertos mensajes con el fin de hacerlos ininteligibles a receptores no autorizados

Sistemas: Un sistema es un objeto complejo cuyos componentes se relacionan con al menos algún otro componente; puede ser material o conceptual.

Aplicaciones: Es un tipo de programa informático diseñado como herramienta para permitir a un usuario realizar uno o diversos tipos de trabajos.

Procedimientos Operativos: son documentos que recogen la interrelación en el tiempo que existen entre diferentes departamentos, normalizando los procedimientos de actuación y evitando las indefiniciones e improvisaciones que pueden producir problemas o deficiencias en la realización del trabajo.

---

[1] Wikipedia. (2018). https://es.wikipedia.org: Acción jurisdiccional. Recuperado de: https://es.wikipedia.org/wiki/Acción_jurisdiccional.

[2] camiloangel.wordpress. (2010). https://camiloangel.wordpress.com: ¿Qué es un activo de información?. Recuperado de: https://camiloangel.wordpress.com/2010/09/03/%C2%BFque-es-un-activo-de-informacion/

[3] Wikipedia. (2019). https://es.wikipedia.org: Acceso a la Información. Recuperado de: https://es.wikipedia.org/wiki/Acceso_a_la_informaci%C3%B3n

Código Malicioso: se trata de un tipo de amenaza que no siempre puede bloquearse con un software antivirus por sí solo.

Copia de Seguridad: es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.

La Transferencia de Archivos: Es decir, es una convención o una norma que controla o permite la transferencia de archivos entre dos o más computadoras o usuarios

Auditoria: Es el examen crítico y sistemático que realiza una persona o grupo de personas independientes del sistema auditado, que puede ser una persona, organización, sistema, proceso, proyecto o producto

Licencia de Software: es un contrato entre el licenciante (autor/titular de los derechos de explotación/distribuidor) y el licenciatario (usuario consumidor /usuario profesional o empresa) del programa informático, para utilizar el software cumpliendo una serie de términos y condiciones establecidas dentro de sus cláusulas.

Titulo

Auditoria de seguridad informática cabildo indígena de corinto alineadas al COBIT 5 e ISO 27001.

1. Pregunta de Investigación

¿Cómo mejorar en el Cabildo Indígena del Resguardo Paéz de Corinto la seguridad de la información?

2. Formulación del Problema

Se ha podido determinar que dentro de la organización existe información “importante o confidencial” ya que ha llegado a manos de personas fuera de la organización y del personal autorizado, con lo cual da a ver que la seguridad de la organización no es adecuada para la protección dela información que resguarda la organización y esto afecta directa e indirectamente al cabildo, esto ha generado cierta preocupación en los mandos administrativos del cabildo de corinto.

El rendimiento de los sistemas de cómputo (computadores) no es el más recomendado para ciertas áreas de trabajo del cabildo de corinto con lo cual no se genera la producción adecuada de cada área de trabajo de la organización.

3. Resumen

Se realizó esta auditoría a la organización del Cabildo Indígena del Resguardo Paéz de Corinto para determinar el nivel de seguridad y protección de la información “importante o confidencial” para así asegurar una optimización de recursos para garantizar el buen funcionamiento de las distintas áreas de trabajo de la organización.

También cabe resaltar que la información ha llegado a manos de personas fuera de la organización y del personal autorizado, con lo cual da a ver que la seguridad de la organización no es adecuada para la protección dela información que resguarda la organización y esto afecta directa e indirectamente al cabildo, esto ha generado cierta preocupación en los mandos administrativos del cabildo de corinto y las autoridades indígenas SA´T WESX que debe de velar por el bienestar o el WET WET FXI´ZENXI de la comunidad Indígena Nasa del Plan de Vida Cxha Cxha Wala(FUERZA GRANDE)

Palabras Claves: Cabildo, SA´T WESX,Nasa,Resguardo,WET WET FXI´ZENXI, Cxha Cxha Wala

4. **Abstract**

This audit was carried out on the organization of the Indigenous Cabildo of the Paéz de Corinto Reservation to determine the level of security and protection of the information "important or confidential" in order to ensure an optimization of resources to guarantee the proper functioning of the different work areas of the organization.

It should also be noted that the information has reached the hands of people outside the organization and authorized personnel, which shows that the security of the organization is not adequate for the protection of information that protects the organization and this directly affects the organization. Indirectly to the cabildo, this has generated some concern in the administrative commanders of the council of corinto and the indigenous authorities SA'T WESX that must watch over the well-being or the WET WET FXI'ZENXI of the Nasa Indigenous community of the Cxha Cxha Life Plan Wala.

Keywords: Cabildo, SA´T WESX,Nasa,Resguardo,WET WET FXI´ZENXI, Cxha Cxha Wala

5. Introducción

Se tomó la decisión de realizar una auditoria en seguridad de la información en el Cabildo Indígena del Resguardo Paéz de Corinto utilizado cobit 5 e iso 27001 cuya principal función es ayudar a que tanto el Software y Hardware disponible en la organización del cabildo no sea vulnerado y que cumpla con todos los estándares de seguridad. Con este fin se quiere mejorar los recursos tecnológicos y su seguridad.

6. **Justificación**

Este proyecto tiene como fin implementar una auditoria de seguridad basada en cobit 5 bajo el esatndar iso 27001 en donde se busca la mejora y el rendimiento para la protección de la información “importante o confidencial” asegurar una optimización de recursos para garantizar el buen funcionamiento de las distintas áreas de trabajo o ya´jas de la organización indígena con la metodología magerit, donde se elaboró una serie de listas de chequeo y entrevistas a los diferentes dinamizadores que están dentro del Cabildo indígena del Resguardo Paéz de Corinto.

Debido a esta auditoria tomar recomendaciones o sugerencias con el fin de que la organización indígena se fortalezca mediante los estándares que se obtiene como entidad para tener una información oprima y confiable sin recibir perjuicios o daños por personal externo.

7. Objetivos

Objetivo General:

Auditar las diferentes dependencias y áreas de trabajo del Cabildo Indígena Paéz de Corinto para determinar su grado de seguridad informática alineado al COBIT 5 e ISO/IEC 27000.

Objetivo Específico:

- Evaluar la seguridad de la información en cuanto a hardware, con procesos de auditoría basada en los estándares COBIT e ISO/IEC 27000, con el propósito de establecer recomendaciones, que permitan la definición de políticas, procesos y procedimientos del Cabildo Indígena del Resguardo Paéz de Corinto este aspecto.
- Evaluar la seguridad de la información en cuanto a software, con procesos de auditoría basada en los estándares COBIT e ISO/IEC 27000, con el propósito de establecer recomendaciones, que permitan la definición de políticas, procesos y procedimientos del Cabildo Indígena del Resguardo Paéz de Corinto en este aspecto.
- Evaluar la seguridad de la información en cuanto a instalaciones, con procesos de auditoría basada en los estándares COBIT e ISO/IEC 27000, con el propósito de establecer recomendaciones, que permitan la definición de políticas, procesos y procedimientos del Cabildo Indígena del Resguardo Paéz de Corinto en este aspecto.
- Presentar el informe final de auditoría con recomendaciones soportadas en hallazgos y evidencias de la ejecución

8. Clase de Investigación

La presente tesis se enmarca dentro la investigación exploratoria ya que se analizar e investigar aspectos concretos de la realidad del cabildo indigena del resguardo paez de corinto en cuestinos de seguridad informática que aún no han sido analizados en profundidad. Por sus características, este tipo de investigación no parte de teorías muy detalladas, sino que trata de encontrar patrones significativos en los datos que deben ser analizados para, a partir de estos resultados, crear las primeras explicaciones completas sobre lo que ocurre.

9. Estado del Arte

Actualmente, en el cabildo indígena del resguardo Paéz de Corinto, no existen estudios, ni investigaciones, como antecedentes al tema de seguridad interna sobre la información y manejo de confidencialidad en la organización, de tal forma, que esta investigación en auditoria es pionera para el programa de ingeniería de sistemas, ya que es la primera de su tipo, que se lleva a cabo.

10. Marco Referencial

10.1. **Antecedentes.**

Entre los trabajos de grado realizados, relacionados con el objeto de estudio se puede mencionar los siguientes:

1. DEFINICIÓN DE POLÍTICAS DE SEGURIDAD INFORMÁTICA PARA EL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO, realizado por María Constanza Torres B. y Efraín Fajardo Guevara. El trabajo consistió en realizar los procesos de auditoría a la seguridad del Centro de Informática de la Universidad de Nariño. Este trabajo tiene relación ya que concientizó al centro de informática en definir políticas de seguridad para que sea más seguro.

2. AUDITORÍA DE SEGURIDAD INFORMÁTICA ISO 27001 PARA LA EMPRESA DE ALIMENTOS “ITALIMENTOS CIA. LTDA.”, realizado por Christian Miguel Cadme Ruiz y Diego Fabián Duque Pozo en la Universidad Politécnica Salesiana Sede Cuenca (Ecuador). El trabajo consistió en aplicar los procesos de auditoría a la seguridad de la empresa

ITALIMENTOS CIA. LTDA. Este trabajo aplicó una norma internacional para realizar el proceso de auditoría.

3. AUDITORÍA INFORMÁTICA DE LA COOPERATIVA DE AHORRO Y CRÉDITO "ALIANZA DEL VALLE" LTDA. APLICANDO COBIT 4.0, realizado por Gabriela Fernanda Barros Marcillo y Andrea Erika Cadena Marten en la Universidad Escuela Politécnica del Ejército (Ecuador). El trabajo consistió en describir la Auditoría Informática de los Sistemas de Tecnología e Información, realizada a la Cooperativa de Ahorro y Crédito "Alianza del Valle". Ltda. Utilizando COBIT, una herramienta desarrollada para, ayudar a los administradores de negocios a entender y administrar los riesgos asociados con la implementación de nuevas tecnologías, las buenas prácticas de COBIT están enfocadas en el ambiente de control óptimo que debe tener una empresa para de esta manera lograr una alineación efectiva entre TI y los objetivos de negocio. El fin de esta revisión técnica es identificar debilidades y emitir recomendaciones que permitan minimizar riesgos.

Este trabajo de grado escogió unos dominios para ser auditados y se aplicó un marco internacional para las prácticas del control de información.

11. **Marco Histórico.**

En los resguardos indígenas en contexto de corinto es un territorio muy amplio además de haber personas con diferentes tradiciones y costumbres es por ello que se necesita saber cómo es los diferentes comportamientos de ellos.

11.1. **Reseña Del Municipio**

Ilustración 1 Escudo y Bandera de Corinto.

Fuente: Alcaldía Municipal de Corinto

En los tiempos de la Colonia existía un vasto territorio al norte del Departamento del Cauca, en donde actualmente se asienta el Municipio de Corinto, Según el historiador Quintana (2011) haciendo referencia a "Don pablo Zúñiga M en una fecha cualquiera del año 1867, Don Antonio Feijoo en función de voluntades con su hermano Don Juan Bautista y unos tantos moradores, llevaron a la practica el proyecto de fundar la población imaginada, y lo hicieron en cuanto al trazado de algunas calles y de la plaza que sería la del mercado. El 11 de mayo del año de 1.868, se le concede la categoría de Municipio de Corinto.

De acuerdo con datos recopilados por el Historiador Quintana (2011), la fundación de Corinto se acredita a Don Antonio Feijoo dueño de la hacienda los "Frisoles", terrenos donde se fundara la población, y su hermano don Juan Bautista Feijoo, quienes vendería a los señores Raimundo Lara, Eulogio Cándelo y Gregorio Rodríguez, las primeras diez y seis cuadras "cuadradas" por un valor de $128 del lugar que hoy se conoce como el municipio de Corinto.

También figuran en, la historia como otros fundadores los señores: "José María Quintero, Juana Ramos, Francisco y Vicente Penagos, Juan Hernández, Gaspar Ramírez, Manuel santos Banguero, Pedro y María Lara (estos últimos considerados por el historiador Thomas Maya en su geografía del departamento del Cauca 1924)

11.2. **El Nombre De Corinto**:

Los participantes de la fundación "resolvieron discutir el nombre de Corinto y San Miguel. Cada domingo, a decir de nuestros viejos informantes, se reunían en la casa de Bernardo Zúñiga, tomada como centro popular y presidida por Don Ramón Vivas S, que tomo a su cargo el bautismo, allí entraban a discutir sobre estos nombres, finalmente se atribuye este nombre a una de las más florecientes ciudades de la antigua Grecia, Corinto qué en otra época se llamó Peloponeso, destruida por los romanos 146 años antes de Cristo

En los tiempos de la Colonia existía un vasto territorio al norte del Departamento del Cauca, en donde actualmente se asienta el Municipio de Corinto, Según el historiador Quintana (2011) haciendo referencia a "Don pablo Zúñiga M en una fecha cualquiera del año 1867, Don Antonio Feijoo en función de voluntades con su hermano Don Juan Bautista y unos tantos moradores, llevaron a la practica el proyecto de fundar la población imaginada, y lo hicieron en cuanto al trazado de algunas calles y de la plaza que sería la del mercado. El 11 de mayo del año de 1.868, se le concede la categoría de Municipio de Corinto.

De acuerdo con datos recopilados por el Historiador Quintana (2011), la fundación de Corinto se acredita a Don Antonio Feijoo dueño de la hacienda los "Frisoles", terrenos donde se fundará la población, y su hermano don Juan Bautista Feijoo, quienes vendería a los señores Raimundo

Lara, Eulogio Cándelo y Gregorio Rodríguez, las primeras diez y seis cuadras “cuadradas” por un valor de $128 del lugar que hoy se conoce como el municipio de Corinto.

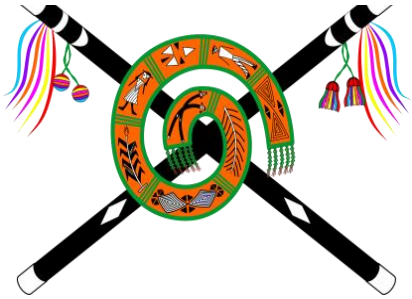
También figuran en, la historia como otros fundadores los señores: “José María Quintero, Juana Ramos, Francisco y Vicente Penagos, Juan Hernández, Gaspar Ramírez, Manuel santos Banguero, Pedro y María Lara (estos últimos considerados por el historiador Thomas Maya en su geografía del departamento del Cauca 1924)

El actual Alcalde del municipio es el señor Edwar García.

12. Marco Contextual

12.1. **Reseña Histórica Del Resguardo**

Ilustración 2. Logo Cabildo



Fuente: Cabildo Indígena de Corinto

12.2. **Época De Colonia**:

Antes de la llegada de los españoles; los pueblos indígenas construían su proyecto de vida en espacios definidos, desarrollando técnicas y acontecimientos acordes con el medio natural y las diferentes necesidades físicas y culturales, eran nómadas, recolectores y cazadores, y luego se convirtieron en sedentarios. Manejaban técnicas complejas de agricultura, alfarería entre otros saberes en lugares y tiempos adecuados.

12.3. **Migración Al Territorio:**

Entre los ríos güengüe y la paila; una tribu pijao a órdenes del Cacique Ocamosa de mucha fuerza y sagacidad fue vencida en el año 1585 por los capitanes españoles LORENZO DE PAZ MALDONADO y ANDRES OCAMPO SALAZAR el territorio en mención es el que hoy ocupa el Municipio de Corinto; esto nos permite afirmar que los primeros habitantes asentados en este territorio a la llegada de la cultura occidental posteriormente fueron los paeces quienes paulatinamente fueron ocupando esta tierras. Esta migración se dio por la presión que ejercieron los españoles contra los paeces en la región de Tierra Dentro, Caldono, Toribio y Jámbalo.

Los paeces llegaron a tierra dentro apenas unos dos siglos antes de enfrentarse a la cultura occidental, por lo tanto, si queremos entender el carácter de la sociedad Páez del siglo XVII es necesario reflexionar sobre los orígenes geográficos de la etnia.

En el siglo XVII es evidente que los paeces mantenían relaciones más estrechas y más cooperativas de las tierras bajas; que, con las tribus de la sierra, tales como los guámbianos. Durante la época de la invasión de España los paeces habitaban dos zonas cerca de la plata y de tierra dentro, además los paeces de la plata quienes habitaban una región más cercana a la selva tropical eran menos rústicos que sus compatriotas de Tierra dentro.

12.4. **Creación de Pequeñas Organizaciones**:

En Colombia a partir del momento que los campesinos empezaron a negarse a pagar terraje y posteriormente a ocupar algunas haciendas, se dan los primeros inicios de la organización campesina en los años 1920-1930; es aquí donde surgen las llamadas “ligas campesinas” que era

una organización que cojia fuerza, pero en la época de la gran violencia en los años 1948 se debilito.

El proceso de organización en el territorio de Corinto no se escapó a las pretensiones de los gobiernos de la época ni a los aspectos generales que vivía el país, es entonces cuando en el año 1969 bajo los argumentos que traía la reforma agraria; que fue creada en 1961 con el fin de contra restar el éxodo de campesinos, la cual no había funcionado desde su creación. Es enviado a Corinto un grupo de personas con el propósito de organizar los campesinos en base a la ley.

De esta última línea llega a Corinto el sacerdote **Pedro León Rodríguez**, quien había sido enviado por el obispo; por segunda vez de manera muy condicionada. Este sacerdote se fue vinculando y apoyando la iniciativa de organización promoviendo el sentido de la unidad y para esto él anduvo en muchas veredas realizando reuniones, orientado la comunidad, creando una conciencia crítica; frente a la vivencia del dominio de los campesinos y los obreros especialmente de la continuidad de la esclavitud; de acuerdo a las pretensiones. También por medio de la iglesia ayudaba a orientar a las comunidades y lo hacía por medio de la misa, reunía la comunidad, pero como todos no eran de confianza, él sacaba solo los líderes de confianza y les daba asesoría después de la misa en la sacristía, de cómo los partidos tradicionales y terratenientes estaban atropellando el pueblo de Corinto, de esta manera él orientaba a los líderes para que de igual forma estos fueran y orientaran la comunidad. Este equipo estaba conformado por el Padre Pedro Leon Rodriguez, Jairo Gamboa,Graciela Bolaños, Ivan Boca Negra, Agustin Fernandes, El Ovispo De Buena Ventura; Valencia Cano, Carlos Enrrique Moreno, quien actualmente vive, y algunos compañeros de otros países como por ejemplo Pablo Tattay, Teresa Tomy (De Chile), Gustavo Soler (argentino) se empiezan a realizar las reuniones que inicialmente se hacían el casa del señor Carlos Enrrique Moreno ubicada en la calle 4 Nº8-

24 del barrió la Playa, Corinto Cauca y posteriormente ingresa Gustavo Mejia, era conocedor y crítico sobre la situación de los indígenas y campesinos del cauca. Después pasa que un montón de personas se reunían constantemente para compartir ideas, y se crea el grupo llamado "Unidad Popular que eran quienes daban las orientaciones de como guiar la comunidad ellos sacaban su propio periódico con el mismo nombre este periódico era para divulgar los hechos y atropellos que se estaban dando en corinto y para informar sobre las cosas buenas que se estaban haciendo. Gustavo Mejía había sido elegido como diputado en el año 1964 por este movimiento, en esta época se tuvieron algunos concejales del mismo movimiento político, estos desempeñaron un papel muy importante, ya que vieron que por medio de la Alcaldía había una posibilidad de exigir tierras para los campesinos luego ingresaron 3 concejales que ayudaron mucho al pueblo.

En ese entonces también ingresan Benjamin Dindicue, Trino Morales, Los Hemanos Avirama, Juan Gregorio Palenchor quienes se ponen en el trabajo de concientizara a las personas; para ellos lograr esto tuvieron que manejar unas estrategias bastante complicadas ya que las reuniones no se podían hacer en público donde todos participaban y opinaban como se hace ahora, la misma fuerza pública los presionaban y ellos siempre buscaron alternativas. Se dice que el señor Gustavo Mejia tenía una casa donde manejaba un taller de arreglar aparatos, pero esto solo era para disimular entonces muchas de las personas que tenían aparatos dañados iban a este lugar para que se los arreglaran y de una vez aprovechaban para ir orientando a los líderes de cómo se iba a trabajar en corinto, de cómo se debían organizar.

Este grupo de personas fue fundamental en el proceso de organización de los campesinos en corinto porque a pesar de que fue contratado para unos fines desde el gobierno, estos se dedicaron a hacer procesos de concientización; Gustavo Mejía estaba convencido de que para

obtener fruto había que preparar personas de la comunidad que lideraran el proceso desde la realidad frente a la desigualdad social y a impulsar la obtención de la tierra de manera forzosa como el de seguir con las invasiones en las grandes haciendas, pues el mecanismo era invadir para luego con el INCORA legalizarlas y organizar los campesinos para una lucha colectiva.

También se conformó una organización campesina de nombre FRESAGRO que significa Frente Social Agrario y de esta manera la organización se fue fortaleciendo. FRESAGRO como organización campesina ha tenido relaciones con otras organizaciones, tenemos el líder relacionado con las negritudes, con los indígenas hacia parte la ANUC (la asociación nacional de usuarios campesinos de Colombia) que fue creada en 1967 y fue la primera organización nacional reconocida por el estado. Se lograron estos vínculos se fortalecieron con los campesinos e indígenas por que las negritudes se negaron hacerles frente a las recuperaciones de tierra.

Después de todos estos avances comienzas las persecuciones y los asesinatos en contra de los líderes entre estos Gustavo Mejia quien fue asesinado en el año 1974 y luego el padre PEDRO leon rodriguez tras estos acontecimientos decae la organización de Fresagro ya que sus líderes principales son asesinados y la comunidad aun no es consiente y se van quedando mientras que los resguardo y otros cabildos van creciendo y finalmente desaparece Fresagro

12.5. **Conformación Organización Indígena**:

En la comunidad Páez de Corinto los primeros intentos de reorganización se dieron en lo que hoy se domina la vereda la Capilla, corregimiento de los Andes, donde se organizó el Cabildo indígena hacia los años 1935 y 1940. En el año 1972 el cabildo se organizó nuevamente en la vereda de Santa Elena asumido una posición de lucha en busca de reivindicaciones sociales principalmente aquellas relacionadas con la ley de la reforma agraria. En el año de 1984 se da la

recuperación de tierras en la hacienda de López Adentro, representando una nueva etapa político organizativo dentro del territorio, con unas connotaciones que trascendieron el proceso de pervivencia cultural de la comunidad Nasa. Surge así el cabildo, con la fuerza de una comunidad que en su nuevo asentamiento pretendía organizarse bajo la expectativa de luchar por la reivindicación de los derechos.

En el año 1990 como ya se había hecho la recuperación de tierras, nace la inquietud de organizar la oficina del cabildo en la zona urbana del municipio de Corinto ya que la visión de los mayores era constituir un resguardo amplio, de esta forma la población urbana reconoce al Cabildo y este empieza a trascender de la recuperación de tierras, al espacio político organizativo. Para fortalecer el proceso político organizativo, se empieza a consolidar el plan de vida y finalmente en la vereda de Santa Elena se le da el nombre de Proyecto Cxhäcxha Wala (Fuerza grande).

En el año 1992 a partir del Proyecto Cxhäcxha Wala se empiezan a construir el plan de desarrollo para Corinto con la participación amplia de la comunidad. En el año 1993 se realiza el estudio socioeconómico para lograr la legalización del resguardo a finales del año ya queda lista la solicitud lo que es un gran avance para el cabildo.

En el año 2007 se entregó al cabildo la parte alta con el título de resguardo, bajo el acuerdo 104 del ministerio del interior y de justicia. En los años 2008 y 2009 con la ampliación del resguardo y los recursos de transferencia del sistema general de participaciones de parte del estado, se definen líneas de trabajo mediante el desarrollo de proyectos identificados por la comunidad.

En la comunidad Páez de corinto los primeros intentos de reorganización se dieron en lo que hoy se domina como la vereda la Capilla, corregimiento de los Andes, donde se organizó el Cabildo indígena hacia los años 1935 y 1940, el gobernador fue el señor Manuel Taquinas este intento lo impulso la iglesia para mantener controlado a los indígenas en pago de diezmo y primicias, el terraje por uso de la tierra y el tributo impuesto por su producción. Al inicio se dio un poco de resultado, pero se fue debilitando por que los indígenas se fueron rebelando y asumiendo estrategias como; el no pagar terrajes, internándose en las montañas, luego surge la gran violencia; y así termino de acabar con todo. (Es importante resaltar que el bastón que portó el exgobernador (Javier Soscue Fiscue- 2014) porta, se encontró enterrado en la vereda de la Capilla en manos de la familia TAQUINAS).

Este intento sirvió como experiencia para los indígenas sobre las estrategias del dominio del hombre blanco, de igual manera se intentó en lo que hoy se conoce como la vereda de Media Naranja, corregimiento de la misma; pero tampoco dio resultados con los terratenientes.

12.6. **Recuperación De Tierras**:

En 1972 el cabildo se organizó nuevamente en la vereda de Santa Elena y el gobernador fue el señor FRANCISCO TALAGA es esta ocasión los indígenas habían asumido una actitud de lucha en busca de reivindicaciones sociales orientadas por el grupo interdisciplinario como se llamó a las personas que el INCORA había enviado contratados para realizar el estudio socioeconómico que exigía la ley de la reforma agraria.

En el año de 1984 se da la recuperación de tierras en López Adentro, donde participo un gran número de comuneros del territorio de corinto y de otros resguardos del departamento del cauca con este acontecimiento se enmarca una nueva etapa político organizativo dentro del territorio

con unas connotaciones que trasciende el proceso de pervivencia cultural de la comunidad Páez. Pues surge el cabildo con la fuerza de una comunidad que en su nuevo asentamiento pretendía organizarse bajo la expectativa de luchar por la reivindicación de los derechos.

Con la recuperación de tierra en López Adentro, donde se solidarizaron otras comunidades de diferentes resguardos, crece la militarización. A raíz de las recuperaciones de tierra y sobre todo el reciente conflicto de López Adentro el cabildo es visto por las autoridades como subversivo invasor.

Después de todo el cabildo sigue funcionado en las comunidades de las tierras recuperadas en la parte plana y tiene su oficina en López Adentro, pero las mismas comunidades de la parte alta no ven con buenos ojos al cabildo y era visto como "roba tierras", "come vacas" "invasores" y castigadores con juete. Ya asentada la comunidad en el reciente territorio recuperado la comunidad se organizó nuevamente y el gobernador fue el señor JULIO TROCHEZ impulsador de la recuperación.

12.7. **Crecimiento De La Organización:**

En el año 1988 a mitad de año se hace un cambio de gobernador (por ser muy débil) y empiezan a entrar unos gobernadores más activos con sueños muy claros los señores: Pedro Ulcue, Miguel Secue, Agustin Noscue Y Marino Calambas.

En el año 1990 con el gobernador AGUSTIN NOSCUE y algunos líderes como ya se había hecho la recuperación de tierras nace la inquietud de trasladar la oficina del cabildo e ir buscando un espacio en Corinto en la zona Urbana ya que la visión de los mayores fue constituir un resguardo amplio y se hablaba de que iba desde el rio güengüe hasta el rio palo colindando con Tacueyó subiendo hasta el páramo y bajando hasta la parte plana; entonces se vio la

necesidad de no quedarse encerrados solamente en López Adentro si no proyectarse hacia la parte alta de Corinto, es decir en la Zona Urbana; Así que el cabildo comienza a hacer delimitación y legalización para no quedarse encerrados en López Adentro y así es que realizan visitas en las comunidades para buscar el dialogo con los presidentes de las juntas para aclarar la situación. Luego de salir de López adentro el cabildo se va a pagar arriendo en una casa en Corinto ya estando allí legalizado podía aplicar la justicia en la parte plana y en corinto también para brindarles un mejor servicios a las comunidades, el cabildo daba remisiones para salud ya que había algunas personas que no tenían dinero para pagar, de igual manera se logró acercamientos y diálogos con la policía y el ejército para hacerles entender la Autoridad Propia y los derechos Indígenas y las comunidades comienzan a aceptar el cabildo poco a poco. El gobernador preocupado porque no tenían fondos para seguir pagando arriendo decide hablar con el padre ESIO lograron conseguir un millón doscientos mil pesos (1´200.000) con esto compraron una casa y así dejaron de pagar arriendo.

En los años 1989 y 1990 el gobernador planteo que: en las comunidades no se podía castigar la gente con juete que se iba a buscar la forma de cambiar esos castigos; en vez de juete seria trabajar en las mismas comunidades y esto dio un buen resultado y ahí es en donde se empieza a hablar de "progreso" de cómo organizarse en adelante porque no habían fondos, además el cabildo en este entonces no era atendido en cuanto a peticiones de auxilios por parte del Municipio de Corinto porque ellos manifestaban que eso pertenecía al Municipio de Caloto.

12.8. **Creación Del Plan De Vida**:

A partir de 1990 la organización del cabildo empieza a trascender en el espacio político organizativo, se dan nuevas perspectivas buscando fortalecer la entidad cultural enfocando en el

espacio de la capacitación y concientización frente a la estructura y políticas del estado, los derechos del indígena y reconocimiento de la identidad cultural. Un nuevo proceso se revive con unas políticas definidas y unas estrategias que la comunidad gradualmente ha ido construyendo y asumiendo en el cual hoy se proyecta para fortalecer el plan de vida de la comunidad y Se continuaba pensando que había que darle un nombre al proyecto comunitario y se debatió en varios lugares como: Guabito, en Chicharronal también se pensó el nombre del proyecto y finalmente en la vereda de Santa Elena lo "bautizan" con el nombre de "PROYECTO CXHÄCXHA WALA", es decir "FUERZA GRANDE".

En el año 1992 mediante las asambleas del "PROYECTO CXHÄCXHA WALA" se empiezan a elaborar el plan de desarrollo para Corinto con la participación amplia de la comunidad y con la asesoría de Rubén Darío Espinoza.

En el año 1993 se realiza el estudio socioeconómico para lograr la legalización del resguardo a finales del año ya queda lista la solicitud lo que es un gran avance para el cabildo.

12.9. **Nacimiento De Organización Regional Y Reconocimiento Organización Local**:

Ilustración 3. CRIC

Fuente: Cabildo Indígena de Corinto

Después de coger fuerza nace ya una organización propia en el año 1971 que es el CRIC (Consejo Regional Indígena del Cauca) en una asamblea que se realizó en el municipio de Toribio con la participación de varios cabildos y terrajeros apoyados desde FRESAGRO y líderes del mismo INCORA con la creación del CRIC empieza una nueva etapa en el proceso de las comunidades indígenas. En el año 1990 tiene un ejecutivo del CRIC el señor: PEDRO ULCUE, quien en su función conoce las asambleas del proyecto global donde se habla de la repartición del presupuesto Municipal. En el mismo año el gobernador AGUISTIN NOSCUE quien es muy activo logra hacer una negociación con el Alcalde de Corinto ALFONSO GOMEZ llamado "Carreto". El gobernador le propone al alcalde que lo apoye para que el cabildo no se quede encerrado en unas pocas veredas y sea reconocido y posesionado oficialmente en Corinto manifestándole que tiene una buena fuerza en su comunidad, el alcalde la dice que hable con el senador HUMBERTO PELAEZ, después de esto pudieron dialogar con el senador y él los apoyo. Es entonces en el año 1990el cabildo es reconocido y posesionado oficialmente por el alcalde de corinto.

En el año 1991 nace la constitución política de Colombia entonces con ello nace la necesidad de orientar a las comunidades o más bien a darles a conocer los derechos que tenían con esta nueva constitución, con esto la comunidad empieza a unirse más y más, en este tiempo se empezó a hablar de proyectos que en otros resguardos ya habían como el proyecto de unidad Páez en miranda, el proyecto nasa, el proyecto Global, entonces hubo la necesidad de buscar apoyos como el padre ANTONIO BONANONI que ha estado pendiente de estas comunidades.

Masacre Del Nilo (Caloto-Cauca)

A finales de 1991 ocurre la tragedia de la masacre del Nilo donde son asesinados 20 compañeros de los cuales la gran mayoría eran de la comunidad del Pilamo, después de 7 años tras un largo proceso de investigación con muertes de quienes estaban detrás de la investigación, en el gobierno de ERNESTO SAMPER PIZANO hace el reconocimiento y se compromete a entregar 15.663 hectáreas a las comunidades indígenas de la Zona Norte del Cauca, esta masacre de igual manera representa el fin de las recuperaciones de tierra por la vía de hechos.

Creación Organización Zonal:

Ilustración 4. Zonal

Fuente: Cabildo Indígena de Corinto

En los años 1994 y 1997 de los cuales los dos primeros años es gobernador LUIS ALBERTO FISCUE y los siguientes dos años MAXIMILIANO CAMPO, por otra parte, nace la ACIN en 1994 la cual nombra al gobernador de Corinto LUIS ALBERTO FISCUE como presidente, este hecho se constituye una dificultad para el cabildo de corinto por que le presidente necesita estar dedicado de tiempo a la ACIN y abandona un poco la comunidad de Corinto.

El 14 de agosto de 1996 el ministerio del interior y de asuntos indígenas otorga bajo la resolución 034 el título de resguardo indígena Páez de corinto López adentro como resguardo

incluyendo la Nevera lo cual fue un gran avance para corinto, esto era importante porque más adelante se podrá tener acceso a las trasferencias de la Nación.

En el año 1997 llegan nuevamente las campañas políticas para la Alcaldía se empiezan a sacar candidatos lo que resulta difícil, se ve entonces la necesidad de volver a elegir como candidato a ADOLFO QUINTANA en contra de HAROL EDUARDO PARRA del partido Liberal. En este mismo año se "logran" recuperar las minas de mármol en la parte alta, las minas estaban en manos de unos empresarios externos entonces la comunidad logra que estas minas queden en la comunidad y empiezan a recibir recursos para el cabildo.

En el año 1998 ingresa como gobernador el señor: CRISTOBAL SECUE, Quien después es asesinado el 25 de julio de 2001, con todo el proceso de lucha de él y los anteriores lideres llegan por primera vez los recursos de transferencias a través de la ley 60 para el resguardo de Corinto López adentro, gracias al hecho de que el dinero de las transferencias debe ser distribuidos por el cabildo con las comunidades según sus usos y costumbres pero son administradas a través de la alcaldía, Cristóbal Secue vivió el momento histórico más fuerte de las recuperaciones de tierra en Corinto y en el Cauca.

Avances y Gobernadores de la Organización:

En el año 1999 ingresa el señor: JOSE EDUARDO TROMPETA que a los 4 meses es sustituido por JULIAN COPAQUE, en el año 2000 ingresa nuevamente como gobernador el señor LUIS ALBERTO FISCUE y en el 2001 el señor JULIO CESAR TUMBO LABIO, en el año 2003 ingresa el señor: MIGUEL COCHA, en el 2004 ingresa el señor: NOE VELASCO, en el 2005 LUIS DANILO SECUE, en el 2006 EVELIO QUIGUAPUMBO que fue reemplazado por EDGAR OCORO, en el 2007 nuevamente LUIS ALBERTO FISCUE, en el

2008 y 2009 nuevamente JULIO CESAR TUMBO, en 2010, el señor JOSE EDUARDO TROMPETA, quien por decisión de la comunidad fue sustituido por JAVIER SOSCUE FISCUE.

En el año 2007 nuevamente hubo un gran avance para Corinto tras las luchas constantes en este año se otorgó para Corinto la parte alta el título de resguardo bajo el acuerdo 104 del ministerio del interior y de justicia.

Ya para el año 2008 de igual manera se amplían los recursos del sistema General de Participación, que sigue siendo un g rana avance.

En el año 1998 el cabildo indígena de corinto realiza un convenio con el Bienestar Familiar, donde se inicia trabajando con 3 escuelas, tras esta entidad ver la gran responsabilidad y compromiso del cabildo, ahora se está trabaja con 21 escuelas, de la institución Educativa de Carrizales ubicada en la vereda de Carrizales, corregimiento de los Andes y Carmencita Cardona de Gutiérrez, ubicada en la Vereda de Rio Negro; Corregimiento de la misma.

En el 2006 Con el CRIC se venía manejando el convenio con la contratación de oferentes.

En el año 2009 la (ONG) DIAOKONNIE katastrophenhiffe que llegan desde otros países para prestar una ayuda Humanitaria, llega al resguardo de Corinto exactamente a la organización indígena, ya que en nuestro territorio el orden público tiene mucha injerencia porque en la gran mayoría de comunidades donde tiene jurisdicción el cabildo se han visto afectadas por los enfrentamientos entre los grupos legales e ilegales Por esta razón DIAOKONNIE katastrophenhiffe ingreso a la organización como un gran apoyo; brindándonos ayudas, dándonos charlas y capacitaciones; de igual manera realizaron muchas dotaciones de implementos para los sitios de asambleas permanentes que se vienen

trabajando desde el programa Jurídico como Cabildo. Las dotaciones se brindaban a las comunidades donde se sentía más fuerte la guerra.

Anteriormente los proyectos y demás programas de salud se financiaban con los recursos de la E empresa del (AIC) a través de contratos que establecía la IPS- ACIN y que solamente se trabajaban con la población afiliada al régimen subsidiado, es decir las personas que tenían el carnet del AIC.

En el 2008 y 2009 con la ampliación de resguardo y los recursos del sistema general de participaciones de parte del estado por la población que aparece certificada por el DANE en planeación Nacional (S.G.P), en el cual hay varias líneas de inversión y entre estas se encuentra el programa de salud del cual se desprenden varios proyectos los cuales apuntan a las políticas que se ha trazado este programa para responder de una manera más eficiente a la comunidad. Entre estos se encuentran: 1- Medicina propia que incluye (rituales mayores, armonización a bastones de Autoridad, apagada del fogón, shakelu, cxapus). 2-Apoyo nutricional adulto mayor, 3-cateos a niños para diagnosticar enfermedades propias y 4-talleres educativos en enfermedades propias y enfermedades occidentales. Con los recursos del SGP se trabajaron estas líneas del 2008 y 2009 en el año 2010 y actualmente ya que mediante el diagnostico que arrojaron los proyectos anteriores se empieza a focalizar en la población más afectada.

En el 2008 de igual manera se estableció un convenio con ACCION SOCIAL que es "tripartito", es decir donde participa la alcaldía, el cabildo indígena de corinto y acción social, en donde las comunidades indígenas reciben un subsidio condicionado, es decir las personas que sean beneficiarias deben participar, activamente en educación y en salud, para el tema de

salud, específicamente crecimiento y desarrollo deben ser niños de 0 a 7 años, para salud de 2 a 11 años de edad, de igual manera cumplir algunos requisitos que exige el cabildo.

En Corinto el Cabildo Indígena es elegido mediante asambleas con personas idóneas propuestas por las comunidades y los cargos son distribuidos mediante el voto secreto, y la distribución de los cargos se realizan de acuerdo a la cantidad de votos obtenidos por cada postulado. A partir del 2009 fue aprobada la elección cada 2 años, antes se realizaba cada año. Y son elegidos por todas las personas mayores de 13 años que se encuentren el listado censal del cabildo indígena.

Actualmente el cabildo indígena lo conforma un representante legal que es (Jesus Edgar Ramos)

El Cabildo Indígena de Corinto es una entidad pública de carácter especial, reconocida como autoridad tradicional dentro del territorio ancestral indígena, fundamentado en nuestro derecho propio (Ley de origen, normas naturales propias), los mandatos de la comunidad como máxima autoridad y las resoluciones de las autoridades tradicionales. Ratificado por la ley 89 de 1890, los derechos reivindicados en la Constitución Política de Colombia de 1991 en los artículos 3,7,63,67,246, 329, 286, 330 y el convenio 169 de la O.I.T. y la ley 21 de 1993; legalizado según resolución número 034 del ministerio del interior de asuntos indígenas.

El Cabildo Indígena de Corinto, para orientar su apoyo en el nivel local, tiene creadas las Ya´jas, que orienta sus acciones en función de dar respuesta frente al mejoramiento de la calidad de vida de la población indígena y campesina que habita el territorio.

La directiva del cabildo actual está conformada en la estructura por las siguientes autoridades tradicionales:

SA’T WE’SX: Gerardo Cuetia Trochez.

SA’T WE’SX: Leonidas Perdomo Canas.

SA’T WE’SX: Oneida Argenis Yatacue.

SA’T WE’SX: Encarnacion Ulcue De Secue.

SA’T WE’SX: Nicolas Noscue Mesa.

SA’T WE’SX: Wilmer Fiscue Noscue.

SA’T WE’SX: Jesus Edgar Ramos.

Ya´Jas O Programas Del Plan De Vida Cxha Cxha Wala

Con la orientación de los mayores, líderes y algunos asesores, se crean los programas para orientar las acciones en las comunidades en el marco del plan de vida.

Ya´Ja Kwesx Kapiyanxi Yat - Programa Educación

Nuestra educación está orientada a garantizar la permanencia cultural, formando personas con principios y valores propios de la cultura establecidos en la Ley de Origen – derecho Propio; e impartiendo una enseñanza intercultural, integral, permanente y de calidad donde prevalezcan los principios culturales, territoriales y del trabajo colectivo para el fortalecimiento de la identidad y la autodeterminación, articulados a la realidad del pueblo Indígena Nasa del Resguardo de Corinto.

En el marco del Plan de Vida Cxha Cxha Wala, las comunidades postularon como mandato, las características y condiciones para el perfil del docente, perfil de la comunidad y perfil del estudiante, definieron que se debe enseñar en las escuelas, como se debe hacer y quiénes son los

encargados de hacer seguimiento, control, evaluación al proceso educativo. En el Plan de Vida están plasmados las necesidades, las dificultades, las problemáticas de igual manera los sueños, los ideales y las esperanzas de un pueblo, donde las metas y los propósitos están enmarcados a corto, mediano y largo plazo, enfocados hacia el buen vivir comunitario. La educación es uno de los pilares fundamentales que ayuda a pensar, resinificar, orientar y volver realidad nuestros sueños, es así como nace el Proyecto Educativo Comunitario PEC, concebido como el corazón o motor del Plan de Vida.

En la actualidad el decreto 2500 de 2010 reglamenta de manera transitoria la contratación de la administración de la atención educativa por parte de las entidades territoriales certificadas, como son los cabildos, autoridades tradicionales indígenas, asociación de autoridades tradicionales indígenas y organizaciones indígenas en el marco del proceso de construcción e implementación del Sistema Educativo Indígena Propio SEIP.

La educación para las comunidades indígenas de corinto es PERMANENTE, es decir se aprende todos los días, además la educación en INTEGRAL, por ello todos los espacios son educativos (asambleas, marchas, reuniones, congresos) entre otros.

La educación debe estar orientada para la VIDA DIGNA DE LOS PUEBLOS, por ello los jóvenes y las comunidades deben ser sensibles a las problemáticas y realidades de las comunidades y entre todos buscar soluciones.

La educación debe conllevarnos hacia la RESISTENCIA y LA PERMANENCIA CULTURAL, es decir tenemos la tarea de orientar las nuevas generaciones con raíces e identidades definidas. Esta debe permitir vivir en equilibrio y armonía, con los seres que nos rodean espiritualmente y terrenalmente.

La educación debe servir para la LIBERTAD y la UNIDAD, es decir que las nuevas generaciones hay que mostrarles el camino, los aciertos y des aciertos, para que tomen decisiones con total conciencia desde una perspectiva comunitaria.

Ya´Ja Kwesx Ew Fxinzxenxi - Programa de Salud

Orienta sus esfuerzos a garantizar el derecho a los servicios de salud, esto tiene que ver con el apoyo al fortalecimiento de la medicina tradicional indígena, como de la aplicación del conocimiento milenario de los The Wala, parteras, sobanderos y pulseadores entre otros dinamizadores. En este orden de ideas se cuenta con una Institución Promotora de Salud Indígena IPS-I SALUD-ACIN, que orienta sus acciones en la promoción de la salud y prevención de la enfermedad, la atención espiritual de la enfermedad, el procesamiento de plantas medicinales y la visita familiar a los hogares indígenas a través de una red de promotores indígenas formados especialmente para la orientación en salud para los pueblos indígenas.

Tejido Justicia y Armonía

Promulga por la defensa del espacio vital, el derecho a la organización y el ejercicio de la justicia propia mediante la aplicación de la jurisdicción especial indígena. Contamos con una Escuela de Formación en Derecho Propio, que aporta al entendimiento y construcción en la aplicación de justicia.

Hace parte de este tejido el área de atención a reclusos que acompaña a los indígenas privados de su libertad en cárceles nacionales como de su aplicación justa para miembros indígenas que violan las normas de convivencia ciudadana y los propios de la cultura Nasa. En la actualidad el área está trabajando en la construcción de un centro de rehabilitación especialmente para indígenas, como una opción para tramitar las sanciones sociales bajo otra jurisdicción.

Tejido Defensa de la Vida

Se trabaja por el respeto a la cultura, nuestras formas organizativas y la vida como esencia dada por el ne´jwex (Creador del hombre, la naturaleza y su relación cósmica en la integralidad).

En este espacio se propende por el ejercicio de los derechos culturales en correspondencia con los derechos humanos. La Guardia Indígena vela por la armonía en el territorio, para ello cuenta con voluntarios que alcanzan los 6.000 guardias que vigilan y previenen las posibles vulneraciones de los derechos humanos, el desequilibrio armónico por causa de los grupos armados que se puedan desarrollar al interior de la comunidad. La orientación y formación política es un componente fundamental para el mantenimiento y sostenimiento de esta estructura que hace parte de la filosofía de la organización indígena.

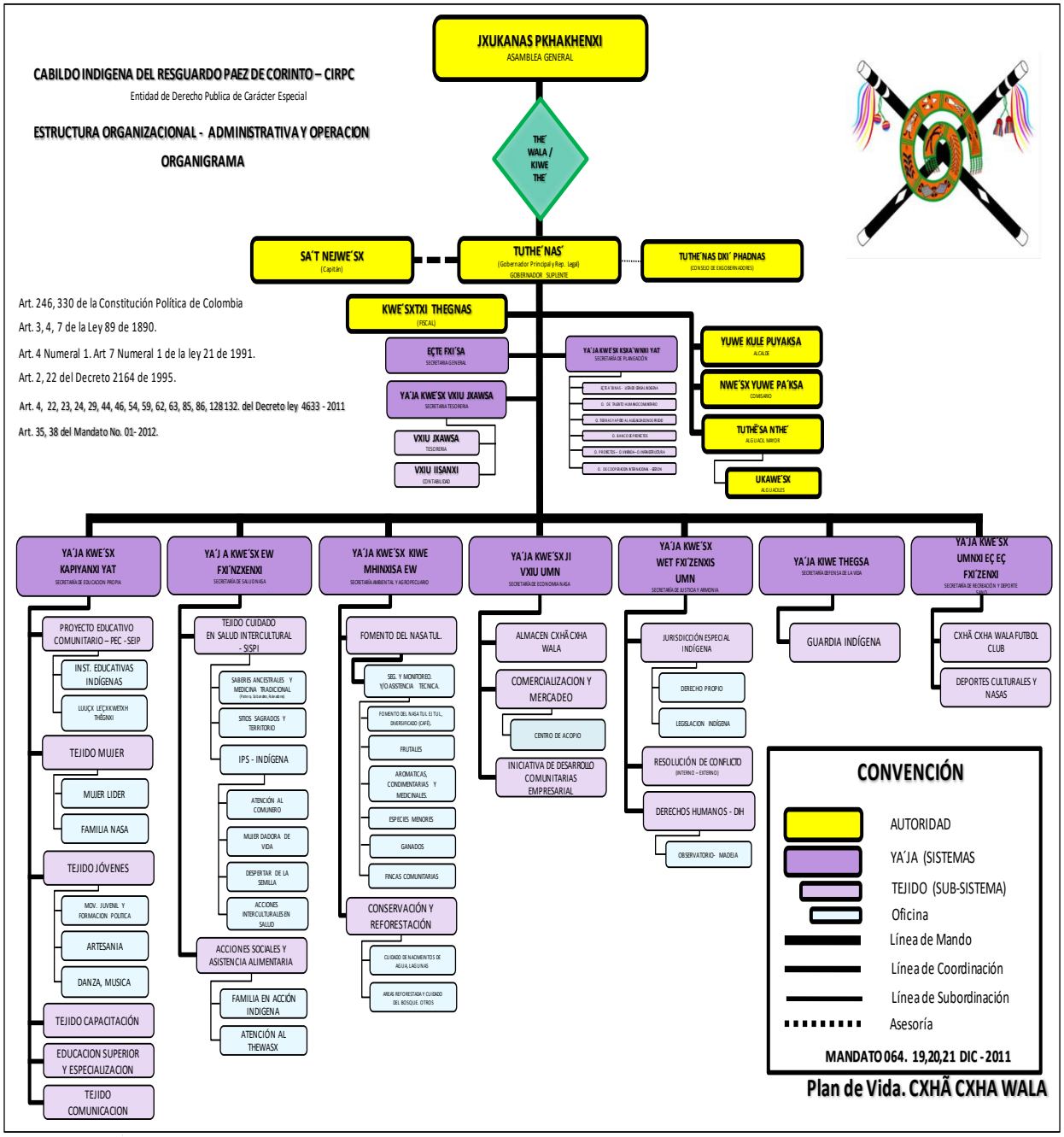
Ya´Ja Ambiental Agropecuario

Centrada en el fortalecimiento de las prácticas ancestrales – tradicionales – de cultivo de plantas y cría de animales, siendo un referente importante la conservación de los recursos naturales (Territorio, bosques, ríos y paramos). Se impulsa formas de producción sostenibles y la aplicación de técnicas y sistemas milenarios como es el Nasa tul o huerta tradicional. Para su operación se ha conformado un área Agro-ambiental con un equipo que impulsa la conservación y el fortalecimiento del sistema de producción tradicional y la aplicación del conocimiento milenario. Se trabaja por el cumplimiento de los acuerdos con el gobierno nacional en relación con la política agraria. Se cuenta con el Centro de Investigación Agroambiental en la comunidad el Nilo, que impulsa la investigación y la adecuación de técnicas apropiadas a las zonas de ladera y la zona plana, donde se investiga, mejora y adaptan semillas vegetales y especies menores de animales.

De igual forma se apoya y desarrolla iniciativas para la comercialización de productos agropecuarios de la zona. La comercializadora realiza acciones de compra de cosechas y venta de productos de primera necesidad en las comunidades.

Estructura organizativa del Cabildo Indígena del Resguardo Paez de Corinto

Ilustración 5. Estructura organizativa del Cabildo Indígena del Resguardo de Corinto.



Misión

Comunidad participa, fortaleciendo sus usos y costumbres, su identidad, apoyando su autoridad tradicional, para la articulación de acciones de emprendimiento e iniciativas comunitarias, conservando los principios de reciprocidad, comunitariedad y solidaridad para el afianzamiento del Plan de Vida Cxha Cxha Wala y la puesta en marcha de los mandatos para alcanzar los resultados anhelados por los habitantes del Territorio Indígena Ancestral y Resguardo Indígena Paéz de Corinto.

Visión

Comunidad Indígena Nasa del Territorio Indígena Ancestral y Resguardo Indígena Paéz de Corinto, alcanzando el WET WET FXI´ZENXI como un principio de la vivencia cosmogónica y cultural de la armonía y el equilibrio natural, reconstruyendo su espacio de vida YAT WALA, mejorando la calidad de vida de su comunidad y trabajando coordinadamente con las autoridades municipal, departamental y nacional para hallar soluciones acorde con su cultura e identidad, hacia la búsqueda de relaciones y cooperación entre la autoridad tradicional en el ejercicio del gobierno propio para la superación de pobreza extrema en el que se encuentra en la actualidad.

13. Marco Conceptual

Auditoría Interna: actividad independiente de una organización que evalúa las actividades contables, financieras y demás operaciones que sirven como base para la organización.

Control Interno: Conjunto de métodos y procedimientos establecidos en una empresa que en forma coordinada tiene entre otros objetivos: la protección de los activos, la obtención correcta de la 8 información financiera, la promoción de eficiencia de operación y la adhesión a las políticas establecidas

Eficacia: significa alcanzar objetivos y resultados. Un trabajo eficaz es aquel que resulta provechoso y exitoso.

Eficiencia: significa hacer las cosas bien y de manera correcta. El trabajo eficiente es un trabajo bien ejecutado.

Auditor: Es un profesional capacitado con total independencia designado para evaluar, obtener evidencia y emitir un juicio coherente sobre procesos determinado de una organización, el auditor dictamina y realizar observaciones con respecto al mejoramiento de eficiencia y eficacia de la organización.

Auditoria De Sistemas: Rama de la auditoria que se encarga de validar la integridad de datos e información almacenada y procesada en Sistemas de Información.

Confidencialidad: Es una propiedad de la información la cual garantiza el acceso únicamente a determinados usuarios o personal dispuesto a preservar el contenido de dicha información.

Integridad: Es una propiedad de la información, la cual busca mantener datos libres de errores y/o modificaciones permitiendo una precisión de los mismos acompañados de un aseguramiento total de dicha información.

Probabilidad: Es una medida de certidumbre que indica que suceda o no determinado proceso o evento.

Riesgo: Es la proximidad de que se dé un posible daño o contingencia.

Sistema De Control Interno (Sci): Conjunto de procedimientos, normas y técnicas de control que se establecen por parte de la Alta Gerencia de las organizaciones para dotar de seguridad los procesos e incluir elementos en términos de eficiencia y eficacia que permiten identificar riesgos.

14. **Marco Legal**

Las instituciones tienen que tener en cuenta los aspectos legales para el apoyo de la formulación de un proyecto, es por esto que esta investigación se apoya desde lo legal en las siguientes leyes, decretos y reglamentos:

LEY ESTATUTARIA 1581 DE 2012: Entró en vigencia la Ley 1581 del 17 de octubre 2012 de PROTECCIÓN DE DATOS PERSONALES, sancionada siguiendo los lineamientos establecidos por el Congreso de la República y la Sentencia C-748 de 2011 de la Corte Constitucional.

DECRETO 1377 DE 2013: Protección de Datos, decreto por el cual se reglamenta parcialmente la Ley 1581 de 2012. Se tuvo en cuenta esta Ley a la hora de saber cuál es el respeto a las condiciones de seguridad y privacidad de la información.

LEY 1273 DEL 5 DE ENERO DE 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado “de la protección de la información y de los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Esta Ley habla de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos, tiene una serie de artículos los cuales hablan de delitos informáticos y permitió conocer algunas infracciones a sistemas de información.

LEY 603 DE 2000: Esta Ley se refiere a la protección de los derechos de autor en Colombia. Recuerde: el software es un activo, además está protegido por el derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales.

Esta Ley obliga a las empresas a presentar un informe del tipo de software que usa la compañía, con el fin de proteger la propiedad intelectual y evitar el incremento de la piratería.

LEY 23 DE 1982: Los autores de obras literarias, científicas y artísticas gozarán de protección para sus obras en la forma prescrita por la presente Ley y, en cuanto fuere compatible con ella, por el derecho común.

15. **Marco Teórico**

El cumulo de información que se maneja al interior de las organizaciones por la implementación de diversas herramientas que se ejecutan de manera continua en sus sistemas de información, bases de datos, aplicativos corporativos y a través de la web, sin dejar de lado los medios físicos donde se almacena la información pertinente a la organización indígena; toda esta información es el insumo propio de la organización para el cumplimento de sus objetivos y metas además de las que se han trazado y de acuerdo a los mandatos de la asamblea comunitaria.

La información tiene además la función de hacer mover de manera operacional la organización indígena, ya que a través de la información que se maneja a diario, mantiene funcionando la organización además permite cierto nivel de progreso gracias a la implantación de mejoras que se pueden lograr con un constante monitoreo en la documentación, así como en la sistematización de todos y cada uno de los procesos operativos y funcionales, teniendo como eje principal la seguridad de la información.

Seguridad De La Información.

En este contexto dado la seguridad de la información se puede definir como un estado de no vulnerabilidad de la información, es decir mantenerla fuera de todo riesgo, daño o peligro.

Las vulnerabilidades es todas aquellas amenazas que tiene el entorno al manipular las informaciones y puedan alterar la información.

Garantizar un nivel de protección total es imposible, debido a que esta información es manipulada por Humanos y siempre existe el factor humano de error que nos deja la ventana libre para cualquier vulnerabilidad; Debería protegerse adecuadamente cualquiera que sea la forma que tome o los medios por los que se comparta o almacene.

Lo importante es enfatizar que la organización del cabildo indígena de Corinto acepte en su misión, visión y objetivos la seguridad informática va a garantizar minimizar daños a la información va a garantizar la continuidad, progreso de la organización y va a dar credibilidad a su asamblea comunitaria del cumplimiento delos mandatos estipulados con una información veraz y oportuna.

Amenazas De La Información.

• Externas: Intrusión a las redes de la organización o instalaciones físicas, por ejemplo: spam, hackers, suplantación de identidad, fraude, espionaje, sabotaje, robo de información, entre otras.

• Internas: Generadas al interior de la organización, principalmente por el conocimiento de los colaboradores y/o trabajadores comunitarios. Ejemplo: Alteración de la información, divulgación de la información, fraudes, robo, sabotaje, uso no autorizados de sistemas informáticos, etc.

• Naturales: son generadas por desastres naturales, como inundaciones, huracanes, terremotos, incendios, etc.

Análisis De Riesgos Informáticos.

Un riesgo informático es el hecho no deseado que suceda con nuestra información, por eso debemos tener claro los riesgos que poseen nuestra información para con eta información saber si se pueden minimizar, eliminar o controlar, para llegar a determinar los riesgos se debe hacer la tarea de determinar, analizar, evaluar y clasificar los activos de información más importantes según la criticidad de los mismos proceso que se llama metodología de análisis de riesgos la cual explicaremos a continuación.

La investigación se soporta en diferentes teorías y conceptos de autores que han indagado y explorado los diferentes temas acerca de la seguridad de la información, auditoría de sistemas, estándares de auditoría, entre otros. A continuación, se describe estos temas.

Seguridad De La Información.

Define la seguridad informática como "Cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema".

La confidencialidad es mantener la seguridad haciendo que solo personas autorizadas pueden ver datos protegidos, el problema de esto en las organizaciones es decidir que es confidencial y quienes tienen el acceso correcto a esto. La disponibilidad hace referencia a la condición de la información de encontrarse a disposición de quienes deben acceder a ella. La integridad busca mantener los datos libres de modificaciones no autorizadas, una amenaza a la integridad de la información de los datos de una organización es un cambio no autorizado a los datos almacenados en un recurso de red o en tránsito entre los recursos.

La Seguridad de la Información abarca la protección tanto de los Sistemas de Información como de las Redes y de los Computadores. Se trata de un continuo desafío, ya que más que un problema tecnológico, constituye hoy en día un elemento clave que posibilita los negocios y permite que las organizaciones puedan llevar a cabo sus objetivos corporativos.

La seguridad de la información se entiende como la preservación de las siguientes características:

Confidencialidad: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

Integridad: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

Disponibilidad: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Ilustración 6. Seguridad de la Información.

2015.Seguridad de la Información. [ilustración]. Recuperado de: http://iberplanet.com/es/wpcontent/uploads/2015/02/caracteristicasI SO27001.png

Adicionalmente, deben considerarse los conceptos de:

Autenticidad: busca asegurar la validez de la información en tiempo, forma y distribución.

Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

Audibilidad: define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

Protección a la duplicación: consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

No Repudio: se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

Legalidad: referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.

Confiabilidad de la Información: la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

A los efectos de una correcta interpretación de la presente Política, se realizan las siguientes definiciones:

Información: se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

Sistema de Información: se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

Tecnología de la Información: se refiere al hardware y software operados por el Organismo o por un tercero que procese información en su nombre, para llevar a cabo una función propia del Organismo, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

Estos conceptos permiten desde el proceso de auditoría en el Cabildo Indígena del resguardo Paéz de Corinto garantizar que la seguridad de la información va ser analizada en todos los aspectos mencionados, para así poder crear un buen trabajo de auditoría.

Una vez abordados estos conceptos de seguridad de la información es fundamental la gestión de la seguridad como elemento administrativo en Cabildo Indígena del resguardo Paéz de Corinto para así poder garantizar la seguridad de sus recursos.

La Seguridad de la Información tiene como fin la protección de la información y de los sistemas de la información del acceso, uso, divulgación, interrupción o destrucción no autorizada. Esta es una de las principales preocupaciones de una empresa, proteger su información.

Asegurar la información clave en el contexto empresarial, en un mundo altamente interconectado, basado en redes sociales y con sobrecarga de información (particularmente instantánea), es un reto para cualquier ejecutivo de seguridad de la información. En este sentido, entender la dinámica corporativa y la forma como la inseguridad de la información se materializa es una competencia estratégica que los responsables de la seguridad de la información deben desarrollar para mantenerse alertas y anticiparse a los movimientos de la inevitabilidad de la falla.

Las buenas prácticas de administración indican que el establecimiento claro de la misión de una organización es indispensable para que todos los funcionarios ubiquen sus propios esfuerzos y los direccionen en bien de la misma. Además, permite elaborar políticas operativas que facilitan el cumplimiento de la misión de la organización, que pueden entenderse como reglas que hay que seguir obligatoriamente.

Es usual que la alta gerencia cometa errores en cuanto a la seguridad de la información de sus organizaciones, como por ejemplo suponer que los problemas desaparecen si se ignoran, no entender cuánto dinero vale su información y que tanto depende la organización de ella, no lidiar con los aspectos operacionales de la seguridad, no entender la relación que existe entre la seguridad y los problemas de funcionamiento y marcha de la organización, entre otros. Si la administración empresarial propone una misión para direccionar estratégicamente la organización, es posible hacer una analogía con la "administración de la seguridad", y es posible entonces ejecutar una "Misión de Seguridad", que "solucione las falencias, ubicando la seguridad informática al mismo nivel que otras actividades sustantivas de la organización, elaborando un plan de seguridad informática clara, promulgando políticas que se derivan de dicha misión y determinando qué mecanismos se requieren para implementar esas políticas".

Ilustración 7. Ciclo De La Implementación De La Administración En Seguridad.

2017. Ciclo. [Ilustración] Recuperado de: https://www.microsoft.com/spain/technet/recurso/articulos/images/rmch0301_big.gif

Una buena administración de seguridad en el Cabildo Indígena del Resguardo Paéz de Corinto, permitirá que la organización indígena empiece a organizar su información y a dar importancia a sus datos e información.

Para poder realizar una buena administración de seguridad es necesario empezar a realizar el proceso de auditoría en Cabildo Indígena del Resguardo Paéz de Corinto, por esta razón se quiere abordar el concepto de auditoría de seguridad de sistemas de información.

Auditoría De Seguridad De Sistemas De Información.

En la actualidad nadie duda que la información se ha convertido en uno de los activos principales de la organización representando las tecnologías y los sistemas relacionados con la información su principal ventaja estratégica. Las organizaciones invierten enormes cantidades de dinero y tiempo en la creación de sistemas de información y en la adquisición y desarrollo de tecnologías que les ofrezcan la mayor productividad y calidad posibles. Es por eso que los temas relativos a la auditoría de las tecnologías y los sistemas de información (TSI) cobran cada vez más relevancia a nivel mundial.

El sistema de información se refiere al almacenamiento, proceso, comunicación, entrada y salida de la información. “Sobre estas funciones elementales y a través del sistema operativo y las aplicaciones, se mantiene la información, se envían los mensajes y se ofrecen los servicios con valor para la organización”.

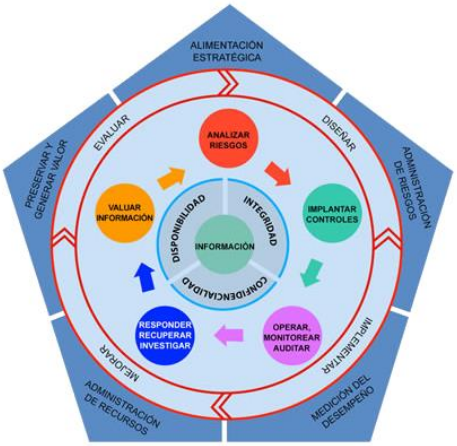
Para ello, se establece un SGSI (Sistema de Gestión de la Seguridad de la Información), que es aquella parte del sistema general de gestión que comprende los recursos necesarios para implantar la gestión de la seguridad de la información en una organización9.

Una auditoría de seguridad informática o auditoría de seguridad de sistemas de información (SI) es el estudio que comprende el análisis y gestión de sistemas, llevado a cabo por profesionales para identificar, enumerar y posteriormente describir las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, redes de comunicaciones o servidores.

Una vez obtenidos los resultados, se detallan, archivan y reportan a los responsables, quienes deberán establecer medidas preventivas de refuerzo y/o corrección siguiendo siempre un proceso

secuencial que permita a los administradores mejorar la seguridad de sus sistemas aprendiendo de los errores cometidos con anterioridad.

Ilustración 8. Auditoria seguridad de la información.



2011. Auditoria. [Ilustración]. Recuperado de: http://www.all4sec.es/w p-content/uploads/2011/09/servicios-consultoria-de-seguridad.png

Las auditorías de seguridad de SI permiten conocer en el momento de su realización cuál es la situación exacta de sus activos de información en cuanto a protección, control y medidas de seguridad.

Fases de una auditoría. Los servicios de auditoría constan de las siguientes fases:

1. Enumeración de redes, topologías y protocolos
2. Verificación del cumplimiento de los estándares internacionales. ISO, COBIT, etc.
3. Identificación de los sistemas operativos instalados
4. Análisis de servicios y aplicaciones
5. Detección, comprobación y evaluación de vulnerabilidades
6. Medidas específicas de corrección

7. Recomendaciones sobre implantación de medidas preventivas

Tipos de auditoría. Los servicios de auditoría pueden ser de distinta índole:

1. Auditoría de seguridad interna. En este tipo de auditoría se contrasta el nivel de seguridad y privacidad de las redes locales y corporativas de carácter interno.

2. Auditoría de seguridad perimetral. En este tipo de análisis, el perímetro de la red local o corporativa es estudiado y se analiza el grado de seguridad que ofrece en las entradas exteriores.

3. Test de intrusión. El test de intrusión es un método de auditoría mediante el cual se intenta acceder a los sistemas, para comprobar el nivel de resistencia a la intrusión no deseada. Es un complemento fundamental para la auditoría perimetral.

4. Análisis forense. El análisis forense es una metodología de estudio ideal para el análisis posterior de incidentes, mediante el cual se trata de reconstruir cómo se ha penetrado en el sistema, a la par que se valoran los daños ocasionados. Si los daños han provocado la inoperatividad del sistema, el análisis se denomina análisis post- mortem.

5. Auditoría de páginas web. Entendida como el análisis externo de la web, comprobando vulnerabilidades como la inyección de código SQL, Verificación de existencia y anulación de posibilidades de Cross Site Scripting (XSS), etc.

6. Auditoría de código de aplicaciones. Análisis del código tanto de aplicaciones páginas Web como de cualquier tipo de aplicación, independientemente del lenguaje empleado.

Realizar auditorías con cierta frecuencia asegura la integridad de los controles de seguridad aplicados a los sistemas de información. Acciones como el constante cambio en las

configuraciones, la instalación de parches, actualización de software y la adquisición de nuevo hardware hacen necesario que los sistemas estén continuamente verificados mediante auditoría.

Estándares De Auditoría Informática Y De Seguridad.

Una auditoría se realiza con base a un patrón o conjunto de directrices o buenas prácticas sugeridas. Existen estándares orientados a servir como base para auditorías de informática. Uno de ellos es COBIT (Objetivos de Control de la Tecnologías de la Información), dentro de los objetivos definidos como parámetro, se encuentra el "Garantizar la Seguridad de los Sistemas".

Adicional a este estándar podemos encontrar el estándar ISO 27002, el cual se conforma como un código internacional de buenas prácticas de seguridad de la información, este puede constituirse como una directriz de auditoría apoyándose de otros estándares de seguridad de la información que definen los requisitos de auditoría y sistemas de gestión de seguridad, como lo es el estándar ISO 27001, serie de normas 27000.

A semejanza de otras normas ISO, ISO/IEC 27000 es un conjunto de estándares desarrollados o en fase de desarrollo por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

Algunas de las normas que conforman la serie 27000 van orientadas precisamente a documentar mejores prácticas en aspectos o incluso cláusulas concretas de la norma ISO/IEC 27001 de modo que se evite reinventar la rueda con el sustancial ahorro de tiempo en la implantación.

ISO/IEC 27000: publicada el 1 de mayo de 2009, revisada con una segunda edición de 01 de diciembre de 2012 y una tercera edición de 14 de enero de 2014. Esta norma proporciona una visión general de las normas que componen la serie 27000, indicando para cada una de ellas su alcance de actuación y el propósito de su publicación. Recoge todas las definiciones para la serie de normas 27000 y aporta las bases de por qué es importante la implantación de un SGSI, una introducción a los Sistemas de Gestión de Seguridad de la Información, una breve descripción de los pasos para el establecimiento, monitorización, mantenimiento y mejora de un SGSI (la última edición no aborda ya el ciclo Plan-Do-Check-Act para

Evitar convertirlo en el único marco de referencia para la mejora continua). Existen versiones traducidas al español, aunque hay que prestar atención a la versión descargada.

ISO/IEC 27001: publicada el 15 de octubre de 2005, revisada el 25 de septiembre de 2013. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 (que ya quedó anulada) y es la norma con arreglo a la cual se certifican por auditores externos los SGSIs de las organizaciones. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI, a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados. Desde el 28 de noviembre de 2007, esta norma está publicada en España como UNE-ISO/IEC 27001:2007 y puede adquirirse online en AENOR (también en lengua gallega). En 2009, se publicó un documento adicional de modificaciones (UNE-ISO/IEC 27001:2007/1M: 2009). Otros países donde también está publicada en español son, por ejemplo, Colombia (NTC-ISO- IEC 27001), Venezuela (Fondonorma ISO/IEC 27001), Argentina

(IRAM-ISO IEC 27001), Chile (NCh-ISO27001), México (NMX-I-041/02-NYCE) o Uruguay (UNIT- ISO/IEC 27001). El original en inglés y la traducción al francés pueden adquirirse en iso.org.

ISO/IEC 27002: desde el 1 de julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Como se ha mencionado en su apartado correspondiente, la norma ISO 27001 contiene un anexo que resume los controles de ISO 27002:2005. Publicada en España como UNE-ISO/IEC 27002:2009 desde el 9 de diciembre de 2009 (a la venta en AENOR). Otros países donde también está publicada en español son, por ejemplo, Colombia (NTC-ISO-IEC 27002), Venezuela (Fondonorma ISO/IEC 27002), Argentina (IRAM-ISO-IEC 27002), Chile (NCh- ISO27002), Uruguay (UNIT-ISO/IEC 27002) o Perú (como ISO 17799; descarga gratuita).

ISO/IEC 27003: publicada el 01 de febrero de 2010. No certificable. Es una guía que se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI de acuerdo ISO/IEC 27001:2005. Describe el proceso de especificación y diseño desde la concepción hasta la puesta en marcha de planes de implementación, así como el proceso de obtención de aprobación por la dirección para implementar un SGSI. Tiene su origen en el anexo B de la norma BS 7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación. En España, esta norma aún no está traducida, pero sí en Uruguay (UNIT-ISO/IEC 27003).

ISO/IEC 27004: publicada el 15 de diciembre de 2009. No certificable. Es una guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles o grupos de controles implementados según ISO/IEC 27001. En España, esta norma aún no está traducida, sin embargo, sí lo está en Argentina (IRAM-ISO-IEC 27004) o Uruguay (UNIT-ISO/IEC 27004).

ISO/IEC 27005: publicada en segunda edición el 1 de junio de 2011 (primera edición del 15 de junio de 2008). No certificable. Proporciona directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001:2005 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. Su primera publicación revisó y retiró las normas ISO/IEC TR 13335-3:1998 e ISO/IEC TR 13335-4:2000. En España, esta norma no está traducida, sin embargo, sí lo está, para la versión de 2008, en países como México (NMX-I-041/05-NYCE), Chile (NCh-ISO27005), Uruguay (UNIT-ISO/IEC 27005) o Colombia (NTC-ISO-IEC 27005).

ISO/IEC 27006: publicada en segunda edición el 1 de diciembre de 2011 (primera edición del 1 de marzo de 2007). Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información. Es una versión revisada de EA-7/03 (Requisitos para la acreditación de entidades que operan certificación/registro de SGSIs) que añade a ISO/IEC 17021 (Requisitos para las entidades de auditoría y certificación de sistemas de gestión) los requisitos específicos relacionados con ISO 27001:2005 y los SGSIs. Es decir, ayuda a interpretar los criterios de acreditación de ISO/IEC 17021 cuando se aplican a entidades de certificación de ISO 27001, pero no es una norma de acreditación por sí misma. El original en inglés puede adquirirse en iso.org. En España, esta norma no está traducida, sin

embargo, sí lo está, para la versión de 2007, en México (NMX-I-041/06-NYCE) o Chile (NCh-ISO27001).

ISO/IEC 27007: publicada el 14 de noviembre de 2011. No certificable. Es una guía de auditoría de un SGSI, como complemento a lo especificado en ISO 19011. En España, esta norma no está traducida.

COBIT 5 (Objetivos de Control para la Información y Tecnologías Relacionadas).

El COBIT es precisamente un modelo para auditar la gestión y control de los sistemas de información y tecnología, orientado a todos los sectores de una organización, es decir, administradores IT, usuarios y por supuesto, los auditores involucrados en el proceso. El COBIT es un modelo de evaluación y monitoreo que enfatiza en el control de negocios y la seguridad IT y que abarca controles específicos de IT desde una perspectiva de negocios.

Las siglas COBIT significan Objetivos de Control para Tecnología de Información y Tecnologías relacionadas (Control Objectives for Information Systems and related Technology). El modelo es el resultado de una investigación con expertos de varios países, desarrollado por ISACA (Information Systems Audit and Control Association).

COBIT, lanzado en 1996, es una herramienta de gobierno de TI que ha cambiado la forma en que trabajan los profesionales de tecnología. Vinculando tecnología informática y prácticas de control, el modelo COBIT consolida y armoniza estándares de fuentes globales prominentes en un recurso crítico para la gerencia, los profesionales de control y los auditores.

COBIT se aplica a los sistemas de información de toda la empresa, incluyendo los computadores personales y las redes. Está basado en la filosofía de que los recursos TI necesitan

ser administrados por un conjunto de procesos naturalmente agrupados para proveer la información pertinente y confiable que requiere una organización para lograr sus objetivos.

Misión Del Cobit

Buscar, desarrollar, publicar y promover un autoritario y actualizado conjunto internacional de objetivos de control de tecnologías de la información, generalmente aceptadas, para el uso diario por parte de gestores de negocio y auditores.

Beneficios Cobit

1. Mejor alineación basada en una focalización sobre el negocio.
2. Visión comprensible de TI para su administración.
3. Clara definición de propiedad y responsabilidades.
4. Aceptabilidad general con terceros y entes reguladores.
5. Entendimiento compartido entre todos los interesados basados en un lenguaje común.
6. Cumplimiento global de los requerimientos de TI planteados en el Marco de Control Interno de Negocio COSO.

Estructura

La estructura del modelo COBIT propone un marco de acción donde se evalúan los criterios de información, como por ejemplo la seguridad y calidad, se auditan los recursos que comprenden la tecnología de información, como por ejemplo el recurso humano, instalaciones, sistemas, entre otros, y finalmente se realiza una evaluación sobre los procesos involucrados en la organización.

La adecuada implementación de un modelo COBIT en una organización, provee una herramienta automatizada, para evaluar de manera ágil y consistente el cumplimiento de los objetivos de control y controles detallados, que aseguran que los procesos y recursos de información y tecnología contribuyen al logro de los objetivos del negocio en un mercado cada vez más exigente, complejo y diversificado.

Dominios Cobit

El conjunto de lineamientos y estándares internacionales conocidos como COBIT, define un marco de referencia que clasifica los procesos de las unidades de tecnología de información de las organizaciones en cuatro "dominios" principales, a saber:

Planificación Y Organización:

Este dominio cubre la estrategia y las tácticas y se refiere a la identificación de la forma en que la tecnología de información puede contribuir de la mejor manera al logro de los objetivos del negocio. Además, la consecución de la visión estratégica necesita ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, deberán establecerse una organización y una infraestructura tecnológica apropiadas.

Adquisición E Implantación: para llevar a cabo la estrategia de TI, las soluciones de TI deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio. Además, este dominio cubre los cambios y el mantenimiento realizados a sistemas existentes.

Soporte Y Servicios: en este dominio se hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad. Con el fin de proveer servicios, deberán establecerse los

procesos de soporte necesarios. Este dominio incluye el procesamiento de los datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación.

Monitoreo: todos los procesos necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control.

Estos dominios agrupan objetivos de control de alto nivel, que cubren tanto los aspectos de información, como de la tecnología que la respalda. Estos dominios y objetivos de control facilitan que la generación y procesamiento de la información cumplan con las características de efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad.

Usuarios

Representante legal: toma decisiones de inversión en TI y control sobre el rendimiento de las mismas, analizar el costo beneficio del control.

Los Usuarios finales (trabajadores comunitarios): quienes obtienen una garantía sobre la seguridad y el control de la informacion que adquieren interna y externamente.

Los Auditores: para soportar sus opiniones sobre los controles de los proyectos de TI, su impacto en la organización y determinar el control mínimo requerido.

Los Responsables de TI: ya que no cuenta la organización con un r3esponsable, la autordad tradicional asumirá los hallazgos y recomendación para identificar los controles que requieren en cada ya´ja de la organización.

También, puede ser utilizado dentro de las empresas y en este caso la organización indígena un responsable del proceso de seguridad de la informacion en el Cabildo de Corinto con suma

responsabilidad de controlar los aspectos de información del proceso, y por todos aquellos con responsabilidades en el campo de la TI la organización.

Características

Orientado al negocio.

Alineado con estándares y regulaciones "de facto".

Basado en una revisión crítica y analítica de las tareas y actividades en TI.

Alineado con estándares de control y auditoría (COSO, IFAC, IIA, ISACA, AICPA).

Principios:

El enfoque del control en TI se lleva a cabo visualizando la información necesaria para dar soporte a los procesos de negocio y considerando a la información como el resultado de la aplicación combinada de recursos relacionados con las TI que deben ser administrados por procesos de TI.

Requerimientos de la información del negocio: para alcanzar los requerimientos de negocio, la información necesita satisfacer ciertos CRITERIOS:

Requerimientos de calidad: calidad, costo y entrega.

Requerimientos fiduciarios: efectividad y eficiencia operacional, confiabilidad de los reportes financieros y cumplimiento le leyes y regulaciones.

Requerimientos de seguridad: confidencialidad, integridad y disponibilidad.

Niveles Cobit

Se divide en 3 niveles, los cuales son los siguientes:

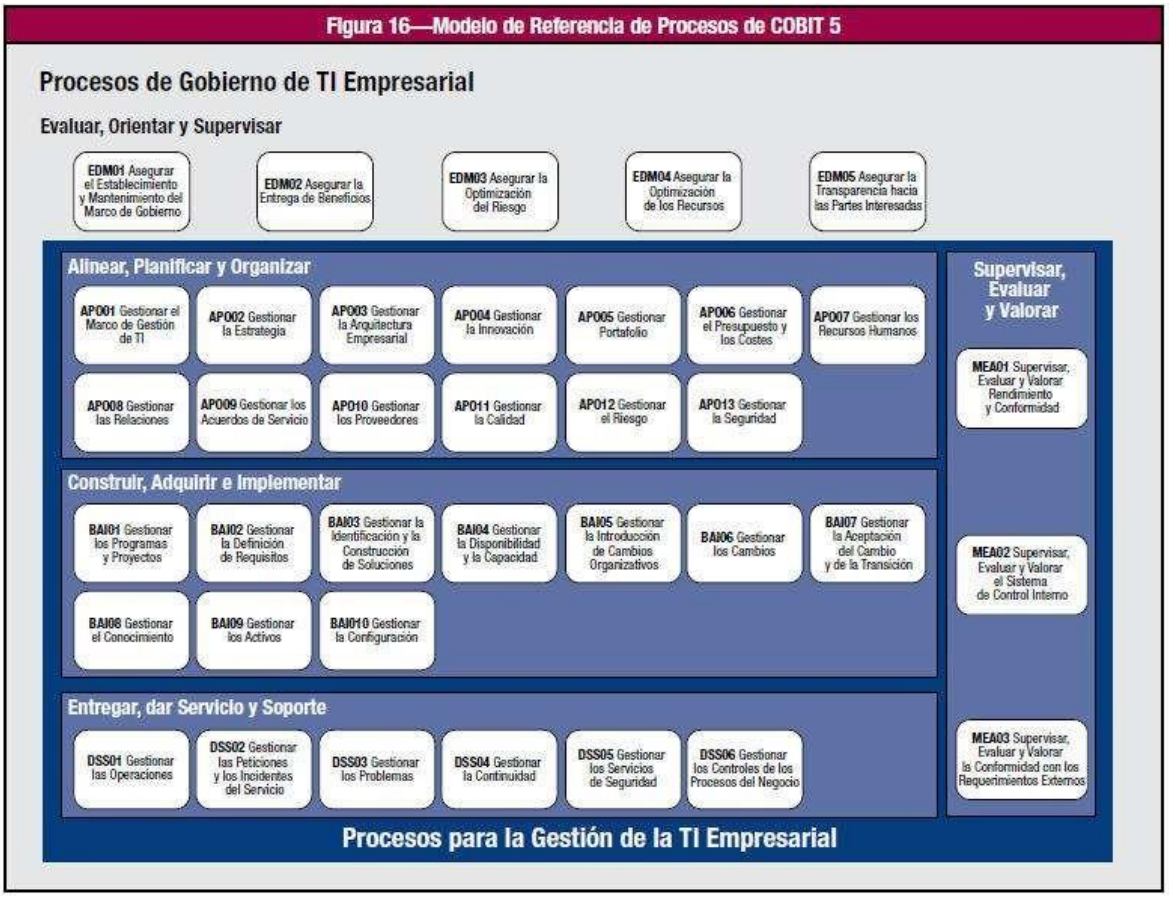
Dominios: agrupación natural de procesos, normalmente corresponden a un dominio o una responsabilidad organizacional.

Procesos: conjuntos o series de actividades unidas con delimitación o cortes de control.

Actividades: acciones requeridas para lograr un resultado medible.

Ya que se esta implementando el COBIT 5 tambien cuenta con procesos agrupados en dominios como lo muestra la siguiente ilustración:

Ilustración 9. Dominios y procesos COBIT 5.



2012. Dominios y Procesos. [Ilustración] Recuperado de: ISACA COBIT 5-2012

Después de realizar una correcta alineación entre COBIT e ISO se debe contar con una herramienta para gestionar los riesgos y para dar un mayor peso a la investigación se utilizó

Magerit.

Es el acrónimo de "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Publicas", creado por el Consejo Superior de Administración Electrónica (CSAE). El uso de esta metodología es de carácter público, pertenece al Ministerio de Administraciones Públicas (MAP) de España.

MAGERIT persigue los siguientes objetivos:

1. Directos: Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.

2. Indirectos: Preparar a la organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

3. El método: realización del análisis y de la gestión, en la planificación del análisis y gestión de riesgos se establecen las consideraciones necesarias para arrancar el proyecto, investigando la oportunidad de realizarlo, definiendo los objetivos que ha de cumplir y el dominio (ámbito) que abarcará, planificando los medios materiales y humanos para su realización e iniciando materialmente el propio lanzamiento del proyecto.

4. Análisis de riesgos: en el análisis de riesgos se identifican y valoran los elementos componentes del riesgo, obteniendo una estimación de los umbrales de riesgo deseables.

Las amenazas según MAGERIT, pueden ser de 4 tipos:

Vulnerabilidades: potencialidad o posibilidad de ocurrencia de la materialización de una amenaza sobre dicho activo.

Impacto: es el daño sobre el activo causado por la amenaza, conociendo el valor de los activos sería muy sencillo calcular el valor del impacto

Riesgo: es la medida de la posibilidad que existe en que se materialice una amenaza. Conociendo el riesgo ya podemos calcular la frecuencia

Salvaguardas: es un mecanismo de protección frente a las amenazas.

Estimación Del Riesgo:

En la medición o estimación de riesgo que se elaboró en el cabildo indígena del Resguardo Paez de Corinto para proveer el grado de peligrosidad y también tener en cuenta el impacto si se genera un riesgo dentro de la organización indígena, en el siguiente cuadro se tiene en cuenta las escalas cuantitativas y cualitativas para tener en cuenta la estimación.

Tabla 1. Escalas Cuantitativas y Cualitativas

IMPACTO	PROBABILIDAD	RIESGO
C: Catastrófico (3)	**A:** Alta (3)	**A:** Alto
M: Moderado(2)	**M:** Media (2)	**M:** Medio
L: Leve (1)	**B:** Baja (1)	**B:** Bajo

Fuente. Magerit version3.0

Tabla 2. Rango de Riesgo

Rango Inferior	**Nivel del Riesgo**	**Rango Superior**
0>=	**B:** Bajo	<=3
3>=	**M:** Medio	<=6
6>=	**A:** Alto	<=9

Fuente. Magerit version3.0

Para obtener la estimación del riesgo es obtenida por medio de la siguiente ecuación matemática:

Riesgo = probabilidad x impacto

Tabla 3. Nivel de Riesgo

		PROBABILIDAD		
RIESGOS		**A:** Alta(3)	**M:** Media (2)	**B:** Baja (1)
IMPACTO	**C:** Catastrófico (3)	A=9	M=6	B=3
	M: Moderado(2)	M=6	M=4	B=2
	L: Leve (1)	B=3	B=2	B=1

Fuente. Magerit version3.0

16. Diseño metodológico

Pasos metodológicos en el proceso de auditoría

La metodología para el proceso de auditoría a Cabildo Indígena del Resguardo Paéz de Corinto consta de las siguientes fases:

Fase I: Planeación

En la fase de planeación se realizaron las siguientes actividades:

- Realizar el estudio inicial en el Cabildo Indígena del Resguardo Paéz de Corinto, para recolectar datos sobre el funcionamiento de la organización.
- Determinar los recursos necesarios para realizar la auditoría.
- Elaboración del plan de trabajo.

Fase II: Ejecución De La Auditoria

En la fase de ejecución se realizaron las siguientes actividades:

- Elección dentro de los dominios del COBIT de los procesos a auditar.
- Ejecutar la auditoría de acuerdo a la metodología (lista de chequeo y entrevistas).
- Elaboración de un análisis de hallazgos y riesgos que permitan identificar cuáles de las actividades identificadas tienen una menor eficiencia, cuáles de los procesos tienen mayor impacto dentro del sistema (ejecución de la auditoría).

Fuentes de recolección de información:

Las fuentes primarias constituyen el objetivo de la investigación bibliográfica o revisión de la literatura y proporcionan datos de primera mano. Las fuentes secundarias son compilaciones, resúmenes y listados de referencias publicadas en un área de conocimiento en particular (son listados de fuentes primarias), es decir reprocesan información de primera mano.

Fuentes primarias. Como recolección de fuentes primarias, con el fin de satisfacer las necesidades inmediatas de investigación en el cabildo indígena del Resguardo Paez de Corinto. Los elementos que se utilizaron para recolectar la información fueron:

- **Listas de chequeo**: se realizara una serie de preguntas al dinamizador comunitario para que pueda responder oralmente o por escrito, con el fin de poner en evidencia determinados aspectos, hallazgos y recomendaciones.

- **Entrevistas:** se utiliza este método con el fin de evidenciar si el dinamizador comunitario tiene el conocimiento sobre la seguridad de la información, en donde se hace una charla amena entre el auditor y el entrevistado.

Fuentes secundarias. Se recopilará una información con anterioridad con el fin de tener una referencia y un punto de partida para desarrollar el proceso de auditoria en el Cabildo Indígena del Resguardo Paéz de Corinto. En donde se tuvo en cuenta lo siguiente

- Datos y documentos suministrados por trabajadores comunitarios del Cabildo Indígena del Resguardo Paéz de Corinto.

- Textos académicos relacionados con la auditoría a la seguridad de la información.

- Temas referentes sobre el proceso de auditoria basado en COBIT e IS0 27001.

Fase III: Consolidación Del Informe Final

- En esta etapa del proceso de auditoría se presenta un informe detallado y especifico a la autoridad y administradores del Cabildo indígena del Resguardo Paéz de Corinto, sustentando donde se dan a conocer los problemas encontrados y se sugieren posibles soluciones.

Resultado Auditoria

Fase 1. **Planeación.**

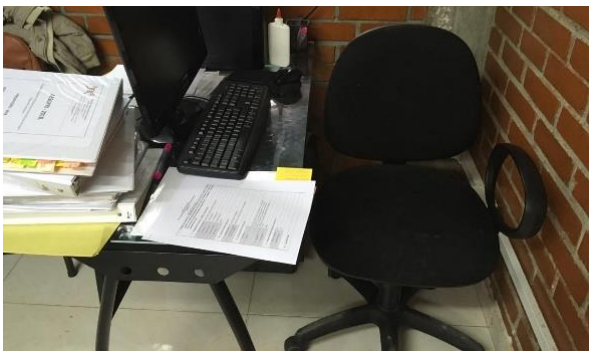
Identificación Del Entorno Auditable

Área Represéntate Legal:

El representante legal es el encargado de la parte administrativa y funcionamiento de la organización como son los convenios con ONG y Gobierno de Colombia, verifica que todos los convenio y acuerdos se cumplan correctamente, además el actual representante legal es parte de los Sat Wesx o autoridades tradicionales ya que son un equipo y cumplen diversas funciones y de acuerdo a sus orientaciones se debe mover la organización ya que ellos son los delegados por la máxima autoridad que la ASAMBLEA CXHA CXHA WALA.

El proceso de auditoría que se ejecutó fueron: la persona, los recursos físicos y tecnológicos de oficina como es equipo de cómputo sistemas operativos.

Ilustración 10. . Área representante legal.



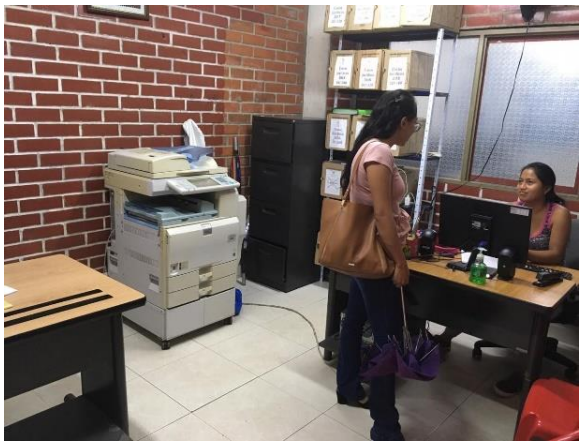
Fuente. Autor auditoria.

AREA E´CTXE FXIZA (SECRETARIA GENERAL):

Esta área es la encargada de recepcionar documento de toda la organización como también define los casos para las áreas encargadas, si son de tipo jurídico, educación, planeación o representante legal, expedir avales y certificados censales.

El proceso de auditoría que se ejecutó fueron: el personal, los recursos físicos y tecnológicos de oficina como es equipo de cómputo y sistemas operativos.

Ilustración 11. Área e´ctxe fxiza



Fuente. Autor auditoria.

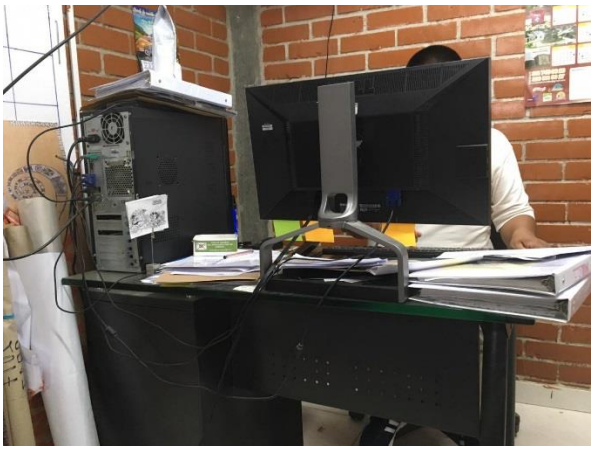
YA´JA KWE´SX KSXA´WNXI YAT (PLANEACIÓN):

El área de planeación se encarda de proyectar y evaluar funciones dentro del CABILDO INDIGENA DEL RESGUARDO PAEZ DE CORINTO, se divide en las siguientes partes:

Coordinador YA´JA:

Es el encargado de planificar toda la estructura y proyecciones del cabildo indígena del Resguardo Paéz de corinto y es quien orienta las partes que hacen parte de esta área como es la de planeación.

Ilustración 12. Área coordinador ya´ja

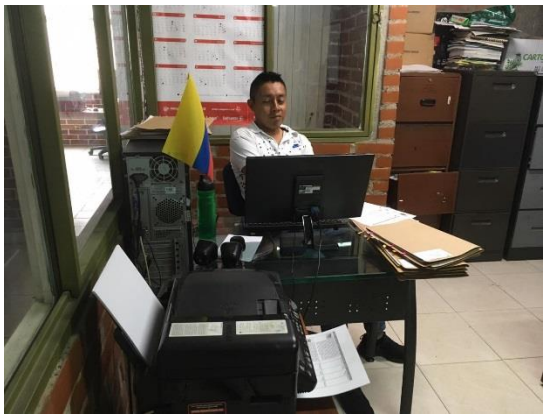


Fuente. Autor auditoria.

Secretario YA´JA:

Es el encargado de recepcionar proyectos y también es el encargado de la parte administrativa para ejecutar lo relacionado con el SGP del resguardo Paéz de corinto y diferentes convenios.

Ilustración 13. Secretario ya´ja.



Fuente. Autor auditoria.

Talento humano YA´JA:

Es la persona encargada del personal que se encuentra laborando dentro de la organización indígena como lo es ya´jas y demás programas que se encuentra bajo la organización del Cabildo Indígena Paéz de Corinto.

Ilustración 14. Talento humano ya´ja.

Fuente. Autor auditoria.

YA´JA KWE´SX VXIU JXAWSA (TESORERIA):

Se encarga de toda la parte financiera y económica además de registrar el recaudo de ingresos diariamente que entra y genera las diferentes ya´jas convenios, SGP, para llevar un control ya que como el gobierno y en este caso las máximas autoridades de la organización rinden cuentas como lo es la ASAMBLEA CXHA CXHA WALA.

Ilustración 15. Ya´ja kwe´sx vxiu jxawsa.

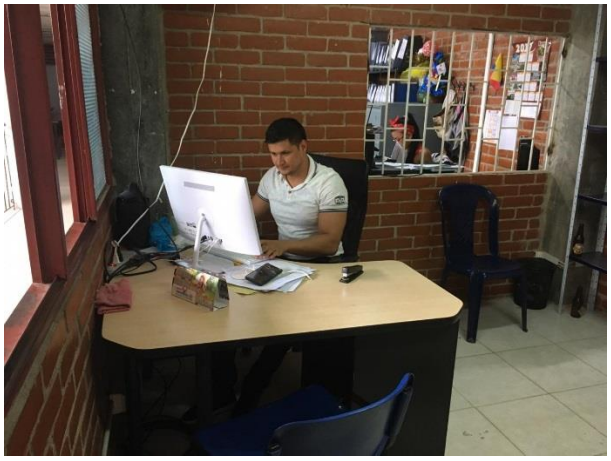
Fuente. Autora auditoria.

VXIU IISANXI (CONTABILIDAD):

Es el encargado de verificar y justificar los ingresos y egresos de la organización en conjunto con la tesorería, Representante legal, autoridad tradicional (SAT WESX), ya que la Asamblea lo delego para que cumpla con esta función tan importante.

El proceso de auditoría que se ejecutó fueron: el personal, los recursos físicos y tecnológicos de oficina como es equipo de cómputo y sistemas operativos.

Ilustración 16. Ya´ja kwe´sx vxiu jxawsa.



Fuente. Autor auditoria.

Ya´Ja Kwesx Kapiyanxi Yat (Educación):

Esta ya´ja es la encargada del futuro de la organización ya que tienen diversas estrategias que van desde la familia, como son niños en la etapa de su vientre hasta sus estudios profesionales, y se divide en las siguientes partes:

Coordinador ya´ja:

La persona encargada de toda la ya´ja quien proyecta y orienta el personal que se encuentra inmerso dentro de esta área que es tan importante dentro del marco del plan de vida indígena.

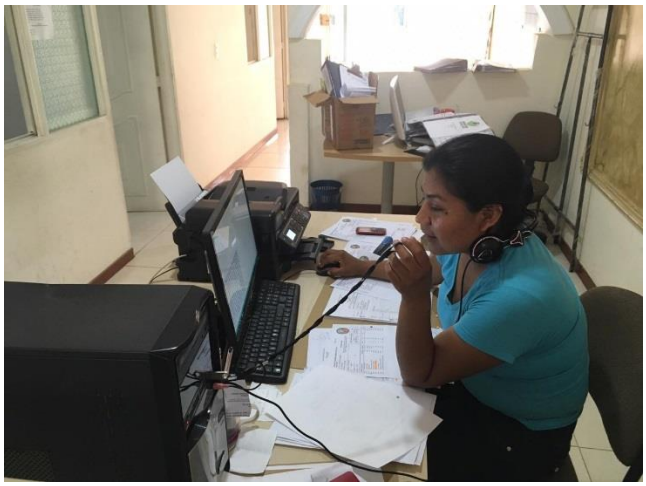
Ilustración 17. Coordinador ya´ja.

Fuente. Autora auditoria.

Secretaria de ya´ja:

Es la persona encargada de recibir documentación que tenga relación con la parte educativa orienta a los dinamizadores en conjunto con el coordinador.

Ilustración 18. Secretaria de ya´ja.



Fuente. Autor auditoria.

Tejido de Comunicación:

Es un equipo de trabajo que hace una labor importante dentro de la organización ya que informa y comunica a través de la radiofrecuencia y además de utilizar instrumentos tecnológicos como son las redes sociales.

Ilustración 19. Tejido de comunicación.

Fuente. Autor auditoria.

Tejido Semillas de vida:

Es un equipo de trabajo quien está encargado de la primera infancia del resguardo Paéz de corinto con base a una educación tradicional indígena.

El proceso de auditoría que se ejecutó fueron: el personal, los recursos físicos y tecnológicos de oficina como es equipo de cómputo y sistemas operativos.

Ilustración 20. Tejido semillas de vida.

Fuente. Autor auditoria.

17. **Plan De Trabajo**:

Objetivo: Evaluar la seguridad informática de la infraestructura tecnológica y sistemas de información en en Cabildo indígena del Resguardo Paez de Corinto.

Alcance: Se evaluará las ya´jas y sus respectivos equipos de cómputo, cumplimiento de las funciones y prestación de servicios, infraestructura física, seguridad física, ubicación, infraestructura eléctrica, redes, Gestión y actualización de la información, Usuarios que acceden al sistema, utilización de la información.

Identificación de Recursos para la Auditoria

En el proceso de auditoria se utilizarán los siguientes recursos:

1. Recursos Humanos: Será realizada por dos estudiantes de la carrera de Ingenierida de Sistemas de la Fundación Universitaria de Popayán.

2. Recursos Físicos: Instalaciones del Cabilo Indigena del Resguardo Paez de Corinto.

3. Recursos Auxiliares: Resma de papel, fotocopias, esferos.

4. Recursos Tecnológicos: Computador Portátil, Memorias USB, Backup en nube.

En el siguiente cuadro se dara a conocer el plan de las actividades a realizar en le proceso de auditoria en cada ya´ja de la organización indígena:

Tabla 4. Plan de actividades.

ACTIVIDADES	FECHA	MATERIALES
Elaboración de listas de chequeo basados en la metodología a implementar.	febrero 2019	Portátil
Visita al Cabildoindigena de las diferentes ya´jas de las Organización. Y su estructura de cómputo.	Febrero 2019	Papelería, esferos y agenda
Entrevista con responsables de cada equipo de cómputo.	Marzo 2019	Papelería, esferos y agenda
Revisión de las Instalaciones físicas por cada ya´ja o área de trabajo.	Marzo 2019	Papelería, esferos y agenda
Identificación de los activos informáticos.	Marzo 2019	Papelería, esferos y agenda

Verificación de horarios de accesos de trabajo.	Marzo 2019	Papelería, esferos y agenda
Niveles de seguridad para el acceso al equipo de cómputo.	Marzo 2019	Papelería, esferos y agenda
Identificación y Evaluación de Riesgos teniendo en cuenta la metodología Magerit	Abril 2019	Portátil, esferos y agenda
Reporte de Hallazgos	Abril 2019	Papelería, esferos, portátil y agenda
Informe Final	mayo 2019	Papelería, esferos, portátil y agenda

Fuente. Autor auditoria.

Fase 2. Ejecución de la auditoria.

Para realizar el proceso de auditoria en el Cabildo Indígena del Resguardo Paéz de Corinto con el estándar de COBIT y su respectivos dominios, procesos y objetivos que se desarrollaran dentro en la auditoria de la organización indígena.

Dominios:

1. Planear Y Organizar (Po)

PO4 Definir procesos, organización y relaciones de TI: Verificar la prestación del servicio, definir roles, funciones y responsabilidades en TI de la institución, establecer las prioridades de los recursos de TI.

PO4.6 Establecimiento de Roles y Responsabilidades

2. Dominio: Adquirir E Implementar (Ai)

AI3 Adquirir y Mantener Arquitectura de TI: mantener y proteger la infraestructuctura tecnológica, mediante de planes que permita la disponibilidad de los recursos.

AI3.2 Protección y Disponibilidad del Recurso de Infraestructura

AI3.3 Mantenimiento de la Infraestructura

3. Dominio: Entregar Y Dar Soporte (Ds)

DS5 Garantizar la seguridad de sistemas: administrar la seguridad para proteger los activos de la institución, establecimiento de controles físicos y lógicos que permitan mejorar el buen uso de los recursos

DS5.2 Plan de Seguridad de TI

DS5.9 Prevención, Detección y Corrección de Software Malicioso

DS12 Administración del Ambiente Físico: establecer controles que proporcione un ambiente seguro y protección contra desastres naturales y fallas humanas que puedan afectar el buen funcionamiento de las instalaciones.

DS12.2 Medidas de Seguridad Física

DS12.4 Protección Contra Factores Ambientales

Recolección De Información Listas De Chequeo Y Entrevista:

Listas de chequeo y entrevistas:

Para la recolección de información de la auditoria en seguridad de la información se implementa la siguiente lista de chequeo y simultáneamente se esta entrevistando y tomando

apuntes relevantes con base a la auditoria de seguridad de la información, para todas las ya´jas o áreas de trabajo del Cabildo Indígena del Resguardo Paéz de Corinto, donde sus respues pueden ser:

SI: cuando se está estableciendo el control.

NO: cuando no se lleva un control.

N/A: no aplica dentro de la organización o ya´ja.

OBSERVACION: se realizarán diferentes casos o anotaciones pertinentes frente al control.

Tabla 5. Lista de Chequeo Roles y Responsabilidades

CABILDO INDIGENA DEL RESGUARDO PAEZ DE CORINTO				
Dominio	**Planear y Organizar**			
Proceso	**PO4 Definir procesos, organización y relaciones de TI**			
Objetivo de Control	PO4.6 Establecimiento de Roles y Responsabilidades: Es necesario establecer un manual de funciones donde se especifiquen los roles y responsabilidades a un dinamizador frente al TI dentro de la organización indígena.			
Cuestionario				
Pregunta	**SI**	**NO**	**N/A**	**OBSERVACIONES**
¿Cuenta la institución con manual de Funciones?				
¿Se establecen los roles y responsabilidades de TI?				
¿Conoce la organización indígena las Funciones en TI?				
¿Hay separación de deberes dentro de la organización?				

Fuente. Autor auditoria

Al desarrollar la lista de chequeo de Roles y Responsabilidades dentro de la organización indígena se encontró:

El Cabildo Indígena del Cabildo Indígena del Resguardo Páez de Corinto no cuenta con un manual de funciones para la utilización de los recursos informáticos dentro de cada ya´ja o área de trabajo de esta organización indígena.

En algunas ya´jas se encuentran roles y responsabilidades como lo son los diferentes dinamizadores comunitarios quienes tiene el manejo de cada equipo de cómputo que les delego la autoridad tradicional (SA´T WESX), pero algunas ya´jas no hay un documento que soporte y establezca las funciones dentro de la misma.

Se encontró que en algunas áreas o ya´jas de trabajo hay deberes y responsabilidades frente a la información y su política de control de los recursos.

Tabla 6. Lista De Chequeo de Protección y Disponibilidad.

CABILDO INDIGENA DEL RESGUARDO PAEZ DE CORINTO				
Dominio	**Adquirir e Implementar**			
Proceso	**AI3 Adquirir y Mantener Arquitectura de TI:** adquirir y proteger la infraestructuctura tecnológica, mediante de planes que permita la disponibilidad de los recursos.			
Objetivo de Control	AI3.2 Protección y Disponibilidad del Recurso de Infraestructura: Establecer controles de protección para asegurar la disponibilidad de los recursos dentro del Cabildo indígena de Corinto.			
Cuestionario				
Pregunta	**SI**	**NO**	**N/A**	**OBSERVACIONES**
¿Existe un inventario identifique los activos de la organización indígena?				
¿Se clasifica la información teniendo en cuenta las responsabilidades?				
¿Hay procedimientos para el manejo de activos?				
¿Hay procedimientos formales para disponer los medios cuando ya no se requieran?				
¿Se protegen los medios físicos que contiene información?				

Fuente. Autor auditoria.

Al desarrollar la lista de chequeo protección y disponibilidad dentro de la organización indígena se encontró:

La organización indígena y algunas dinamizadores comunitarios no tienen conocimientos que hay otros elementos que hacen parte de los activos informáticos, para ellos solo son los computadores, por lo cual no tiene un inventario real de sus activos.

Hay clasificación de la información por las responsabilidades de los dinamizadores dentro cada ya´ja, como también al sistema de información, hay clasificación en donde cada persona maneja su información de acuerdo a su desempeño comunitario.

No hay procedimientos para el manejo de los activos, ni para disponer de los medios cuando no se requieran, no hay protección de los medios físicos que contiene información porque en ocasiones de pierde información importante para el Cabildo indígena de Corinto.

Tabla 7. Lista de chequeo Mantenimiento de Hardware y Software.

CABILDO INDIGENA DEL RESGUARDO PAEZ DE CORINTO				
Dominio	**Adquirir e Implementar**			
Proceso	**AI3 Adquirir y Mantener Arquitectura de TI:** adquirir y proteger la infraestructuctura tecnológica, mediante de planes que permita la disponibilidad de los recursos.			
Objetivo de Control	AI3.3 Mantenimiento del Hardware y Software: Establecer los procedimientos para el mantenimiento del Hardware y software en cada equipo de cómputo en las ya´jas del Cabildo de Corinto.			
Cuestionario				
Pregunta	**SI**	**NO**	**N/A**	OBSERVACIONES
¿Se realiza mantenimiento periódico a los computadores de cada ya´ja?				
¿Existe un cronograma de Mantenimiento a los equipos de cómputo?				
¿Realiza el mantenimiento alguien de la organización indígena?				

Fuente. Autor auditoria.

Al desarrollar la lista de chequeo mantenimiento de hardware y software dentro de la organización indígena se encontró:

Dentro cada ya´ja no se realiza mantenimiento periódico, la persona que está encargada a veces no tiene conocimientos necesarios para realizarla.

No existe un cronograma para el mantenimiento periódico de hardware y software de las áreas o ya´jas del Cabildo de Corinto, cuando hay muy esporádicamente se realiza el mantenimiento, y lo realizan personas ajenas a la organización

Tabla 8. Lista de Chequeo Prevención y Detección de Software Maliciosos

CABILDO INDIGENA DEL RESGUARDO PAEZ DE CORINTO				
Dominio	**Entregar y Dar Soporte**			
Proceso	**DS5 Garantizar la seguridad de sistemas:** administrar la seguridad para proteger los activos de la organización, establecimiento controles físicos y lógicos que permitan mejorar el buen uso de los			
Objetivo de Control	DS5.9 Prevención, Detección y Corrección de Software Malicioso. Establecer las medidas preventivas y correctivas para proteger el hardware y el software de la organización indígena contra malware (virus, gusanos, spyware, correo basura).			
Cuestionario				
Pregunta	**SI**	**NO**	**N/A**	**OBSERVACIONES**
¿Tiene plan para protección de registros?				
¿Hace control para evitar la propagación de código Malicioso?				
¿Se establece condiciones y términos de servicios?				
¿Utiliza medida de protección de los contra código malicioso?				
¿Existe Manual de procedimientos documental?				
¿Existe manual de políticas de respaldo de la información?				
¿Cuenta la institución con antivirus legalizado y dentralizado?				

Fuente. Autor auditoria.

Al desarrollar la lista de chequeo prevención y detección de software maliciosos dentro de la organización indígena se encontró:

Algunas ya´jas no cuentan con un plan de protección de los registros, solo los ingresan al sistema de información y se trabaja según lo requerido por la organización, pero no tiene el control total de los datos ya que alguna información se pierde o se daña por software dañinos.

Hay establecimiento de términos y condiciones para el manejo de la información y los recursos.

No existe control para evitar la propagación de código malicioso porque es lo que frecuentemente ocurre dentro del Cabildo Indígena del Resguardo Paéz de Corinto y es la mayor causa del deterioro de los computadores por la presencia de virus. Por lo cual en algunas ya´jas no cuentan con una medida de protección para evitar su propagación.

El manual de procedimientos, ni manual de política de respaldo no existe dentro de la organización.

La organización no cuenta con un antivirus legalizado.

Tabla 9. Lista de Chequeo Plan de Seguridad de TI.

CABILDO INDIGENA DEL RESGUARDO PAEZ DE CORINTO				
Dominio	**Entregar y Dar Soporte**			
Proceso	**DS5 Garantizar la seguridad de sistemas:** administrar la seguridad para proteger los activos de la organización, establecimiento controles físicos y lógicos que permitan mejorar el buen uso de los recursos.			
Objetivo de Control	DS5.2 Plan de Seguridad de TI: Establecimiento del plan de Seguridad informática que garantice la disponibilidad, confidencialidad e integridad de la información de cada ya´ja en su equipo de cómputo.			
Cuestionario				
Pregunta	**SI**	**NO**	**N/A**	**OBSERVACIONES**
¿Cuenta el Cabildo Indigena de Corinto con política de seguridad de la información, que incluya aspectos físicos				
¿Se da a conocer la política de seguridad de la Información a los dinamizadores comunitarios de la				
¿Se revisa las políticas para seguridad de la información?				

Fuente. Autor auditoria.

Al desarrollar la lista de chequeo plan de seguridad de TI dentro de la organización indígena se encontró:

En una ya´ja del Cabildo de Corinto tiene el conocimiento sobre las políticas de seguridad y cualifica ah algunos dinamizadores sobre este tema cada año, pero las demás áreas les falta adquirir el conocimiento sobre las política de seguridad de la información.

Tabla 10. Lista de Chequeo Medidas de Seguridad Física.

CABILDO INDIGENA DEL RESGUARDO PAEZ DE CORINTO				
Dominio	**Entregar y Dar Soporte**			
Proceso	**DS12 Administración del Ambiente Físico:** establecer controles que proporcione un ambiente seguro y protección contra desastres naturales y fallas humanas que puedan afectar el buen funcionamiento de las instalaciones.			
Objetivo de Control	DS12.2 Medidas de Seguridad Física: Establecimiento de controles de seguridad física.			
Cuestionario				
Pregunta	**SI**	**NO**	**N/A**	**OBSERVACIONES**
¿Se ha establecido controles de seguridad física?				
¿Tiene plan ante la falla del sistema de seguridad?				
¿Se registran las personas que ingresan a las instalaciones de la Organización				
¿Se encuentra definido el perímetro de seguridad física?				
¿Existe política de control de Acceso a las instalaciones?				
¿Hay mecanismos de protección frente a amenazas externas?				
¿Se trabaja en áreas seguras?				
¿Hay política de equipos desatendidos?				
¿Se controla el retiro de activos en el Cabildo de Corinto?				

Fuente. Autor auditoria.

Al desarrollar la lista de chequeo medidas de seguridad física dentro de la organización indígena se encontró:

No cuenta con parámetros de seguridad física que garantice la seguridad de las ya´jas de la organización.

El Cabildo de Corinto no cuenta con un plan ante la falla del sistema de seguridad.

La organización no cuenta con un control y registro de las personas que ingresan a las instalaciones del Cabildo de corinto.

La organización No cuenta con un perímetro de seguridad de las diferentes áreas y ya´jas que se encuentran funcionando dentro del Cabildo.

No hay una política de control de acceso a las instalaciones de esta organización indígena por desconocimiento.

Para la protección frente amenazas externas, esta organización cuenta con alguaciles o AT´X PXUSNXAS y además cuentan con algunos guardias que vigilan las instalaciones, expresan que toda la comunidad y los trabajadores comunitarios prestan la labor de protección ya que esta organización indígena es de la comunidad. Por ende, se considera un área segura.

La entidad no cuenta con una política y procedimientos para los equipos desatendidos, pero los dinamizadores comentan que todos cuidan y controlan el retiro de activos de la organización, pues estos se han adquirido con un esfuerzo y proceso de lucha de toda la comunidad del Resguardo de Corinto.

Tabla 11. Lista de Chequeo Protección de Factores Ambientales

CABILDO INDIGENA DEL RESGUARDO PAEZ DE CORINTO				
Dominio	**Entregar y Dar Soporte**			
Proceso	**DS12 Administración del Ambiente Físico:** establecer controles que proporcione un ambiente seguro y protección contra desastres naturales y fallas humanas que puedan afectar el buen funcionamiento de las instalaciones del			
Objetivo de Control	DS12.4 Protección Contra Factores Ambientales: Establecer políticas de control de acceso al aula de informática para proteger contra factores ambientales.			
Cuestionario				
Pregunta	**SI**	**NO**	**N/A**	**OBSERVACIONES**
¿Existe detector de Humo?				
¿Hay control de Seguridad de acceso a lugares restringidos?				
¿Se ha encontrado alguna falla en el				
¿Se trabaja en áreas seguras?				
¿Existe protección del cableado de energía eléctrica y de telecomunicaciones?				
¿Cuenta las instalaciones con espacio amplio para facilitar la movilización?				
¿Existe señalización de zonas de				
¿Existen extintores?				
¿Existe Sistema de ventilación?				
¿Cuenta la organización con avisos de prohibición de fumar, comer, e ingresar líquidos al área de equipos de cómputo?				
¿Se le hace seguimiento a las				
¿Existe esquema de conexión eléctrica con interruptores?				

Fuente. Autor auditoria.

Al desarollar la lista de chequeo medidas de seguridad fisica dentro de la organización indígena se encontró:

Las instalaciones del Cabildo de Corinto no cuentan con un detector de humo.

Falta de zonas marcadas con acceso restringido en algunas áreas o ya´jas de la organización, puesto que toda persona que ingrese ingresaría fácilmente a cualquier instalación.

En algunas ya´jas e instalaciones son zonas seguras ya que cuentan con un protocolo en caso de algún riesgo presentando se activa una ruta para los dinamizadores comunitarios.

La protección del cableado eléctrico, hay equipos de cómputo que pueden generar un corto ya que no tienen un cableado bien estructurado, y además no encuentran en mantenimiento dentro de esta organización indígena.

En algunas áreas o ya´jas no cuentas con un espacio óptimo y amplio que facilite la movilización en ocasiones se observa que es muy estrecha en comparación a la cantidad de dinamizadores comunitarios dentro de una misma oficina.

Dentro del cabildo de Corinto cuentan con un extintor, el cual se dicta capacitaciones de cómo se utiliza en caso de alguna emergencia.

La organización cuenta con una buena señalización de la zona de evacuación.

La entidad indígena no cuenta con aire acondicionado.

El Cabildo Indígena del Resguardo Paez de Coritno carece de avisos de prohibición de fumar, comer e ingresar líquidos a la zona de equipos de cómputo, ya que alguos dinamizadores comunitarios desconocen el riesgo de dichos eventos teniendo en cuenta el procedimiento formal para estas restricciones.

Todas las ya´jas de la organización cuentan con un esquema de conexión eléctrica con interruptores, reguladores o UPS, dentro de cada oficina y ya´ja del Cabildo de Corinto.

Identificación de Activos:

Para la identificación de activos se toma en cuenta a los entrevistados, que son los dinamizadores comunitarios por cada ya´ja o área de trabajo y se realiza un cuadro en general de activos que cuenta la organización indígena como es en este caso el Cabildo Indígena del Resguardo Paez de Corinto.

Tabla 12. Activos de la Organización.

Tipo de activo	Descripción
Hardware	Computadores de Escritorio que se maneja dentro de las instalaciones o ya´jas
Datos/ Información	Dinamizadores comunitarios, aplicativos y autoridad tradicional.
Software	Apps (contables, organizacionales) Sistema Operativo Windows
Redes de Comunicaciones	Switche Red cableada e inalámbrica (internet)
Equipamiento	Extintor Video Beam
Seguridad Física	Cableado Estructurado Instalaciones Instalaciones eléctricas
Talento Humano	Sa´t Wesx, dinamizadores comunitarios (coordinadores, secretarios(as), apoyos administrativos)

Fuente. Autor auditoria.

Identificación de amenazas.

Según la metodología magerit identificación de las siguientes amenazas en el siguiente cuadro:

Tabla 13. Amenazas Segun Magerit 3.0.

Recursos Afectados	**Amenazas**	**Dimensiones Seguridad**
Hardware	[N.1] Fuego: incendio	Disponibilidad
	[N.*] Desastres naturales	Disponibilidad
	[I.5] Avería de origen físico o lógico:	Disponibilidad
	[I.6] Corte del suministro eléctrico	Disponibilidad
	[I.7] Condiciones inadecuadas de temperatura o humedad: Fuegos de calor	Disponibilidad
	[E.23] Errores de mantenimiento / actualización de	Disponibilidad
	[E.25] Robo	D]
	[A.26] Ataque destructivo	[D]
Software	[I.5] Avería de origen físico o lógico	Disponibilidad
	[E.1] Errores de los usuarios	[I] integridad [C]
	[E.8] Difusión de software dañino: propagación de	[D] disponibilidad
	[E.20] de los programas (software)	[I] integridad [D]
	[E.21] Errores de mantenimiento / actualización de	[C] [I] integridad [D]
Datos	[E.1] Errores de los usuarios	[I] integridad [C]
Equipamiento Auxiliar	[N.1] Fuego: incendio	Disponibilidad [D]
	[N.*] Desastres naturales	Disponibilidad
	[I.5] Avería de origen físico o lógico:	Disponibilidad
	[I.6] Corte del suministro eléctrico	Disponibilidad

	[I.7] Condiciones inadecuadas de temperatura	Disponibilidad
	o	
	[E.23] Errores de mantenimiento / actualización	Disponibilidad
	de	
	[E.25] Robo	D] disponibilidad
	[A.26] Ataque destructivo	[D] disponibilidad
	[A.26] Ataque destructivo	[D] disponibilidad
Instalaciones	[N.1] Fuego: incendio	Disponibilidad
	[N.*] Desastres naturales	Disponibilidad
	[E.7] Deficiencia en las organizaciones	Disponibilidad
Personal	[A.28] Indisponibilidad del personal	[D] disponibilidad

Fuente. Magerit 3.0 Amenazas.

Estimación del Riesgo

Para obtener la estimación de riesgo tendremos en cuenta la frecuencia de ocurrencia del riesgo, el impacto basado en los siguientes aspectos o criterios:

Tabla 14. . Frecuencia de Riesgo.

Frecuencia	
Muy frecuente	**MF**
Frecuente	**F**
Normal	**FN**
Poco frecuente	**PF**

Fuente. Autor auditoria.

Tabla 15. Impacto de Riesgo

Impacto	
Muy alto	**MA**
Alto	**A**
Medio	**M**
Bajo	**B**
Muy bajo	**MB**

Fuente. Autor auditoria.

Tabla 16. Valoración de Riesgo.

Recursos Afectados	**Amenazas**	**Impacto**				**Riesgo**
		D	**I**	**C**	**F**	
Hardware	[N.1] Fuego: incendio	MA	B	B	PF	**B**
	[N.*] Desastres naturales	MA	MB	MB	PF	**B**
	[I.5] Avería de origen físico o lógico:	MA	B	B	F	**A**
	[I.6] Corte del suministro	A	B	B	F	**A**
	[I.7]Condiciones inadecuadas de temperatura o humedad: Exceso de	A	B	B	F	**M**
	[E.23] Errores de mantenimiento / actualización de equipos	MA	M	M	NF	**A**
	[E.25] Robo	A	B	A	PF	**M**
	[A.26] Ataque	A	B	B	PF	**B**
	[I.5] Avería de origen	MA	B	B	F	**A**
Software	[E.1] Errores de los Usuarios	B	A	A	PF	**A**
	[E.8] Difusión de software dañino:	MA	MA	MA	MF	**MA**
	[E.20] Vulnerabilidades	MA	A	A	F	**A**

	[E.21] Erroresde mantenimiento/actualizació n de programas (software)	A	A	B	F	**A**
Datos	[E.1] Errores De los usuarios	A	A	A	N	**A**
	[N.1] Fuego: incendio	MA	B	B		**B**
	[N.*] Desastres naturales	MA	MB	MB	F	**B**
	[I.5] Avería de origen físico o lógico:	MA	B	B		**A**
	[I.6] Corte del	A	B	B		**A**
Equipa miento Auxiliar	[I.7] Condiciones inadecuadas de temperatura o humedad: Exceso de calor	A	B	B		**M**
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	MA	M	M	F	**A**
	[E.25] Robo	A	B	A		**M**
	[A.26] destructivo	A	B	B	F	**B**
	[A.26] destructivo	A	B	B	F	**B**
Instalaci ones	[N.1] Fuego: incendio	MA	B	B		**B**
	[N.*] Desastres naturales	MA	M B	MB	F	**B**

Personal	[E.7] Deficiencia en las Organizaciones	MA	B	B	N	**M**
	[A.28]Indisponibilidad del personal.	A	M B	MB	N	**M**

Fuente. Autor auditoria.

Fase 3. Consolidación E Informe Final

18. HALLAZGOS Y RECOMENDACIONES

Hardware.

El hardware evaluado en el Cabildo indígena del Resguardo Paéz de Corinto fueron los equipos en donde la organización labora diariamente y los más importantes, para ello se realizó una lista de activos, después se clasifico estos activos para determinar su de importancia y además se comprobó de manera particular cuales son las amenazas más significativas que puede sufrir estos activos para realizar una evaluación del riesgo.

En general, el hardware administrado en la organización indígena en sus proyecciones poco a poco gana y gestiona equipamientos como también se realiza esporádicamente un mantenimiento periódico y preventivo en caso de algún fallo y se manipula de acuerdo a la importancia que se requiere.

Recomendaciones: se debe realizar la verificación de hardware y software para garantizar la compatibilidad que se requiere en cada ya´ja. Además, se debe contar con la documentación antes de la evaluación de los requerimientos de la organización.

Software.

El Cabildo Indígena del Resguardo Paéz de Corinto no se dedica al desarrollo de software, por este motivo se determinó cuáles son los programas más utilizados y que se requieren dentro de la misma, como es el procedimiento para la adquisición de software especializado y cuáles son las licencias de los programas que ellos usan.

En conclusión, el software administrado en la Organización se requiere de más gestión para la adquisición de los programas especializados con sus respectivas licencias, debido a que la organización no cuenta con suficientes recursos ha realizado un mantenimiento eficaz y se manipula para cumplir las diferentes labores y responsabilidades.

Recomendaciones: se debe tener una persona encargada de toda el área de Tecnología de Información para realizar un mantenimiento preventivo a recursos TI, para así asegurar que estos funcionen correctamente y no presenten fallos a la hora del uso además, debe asegurar la información instalando software especializado para prevenir spyware y malware en los computadores.

Nombrar a un jefe de sistemas que este responsable de la información y crear políticas de instalación de software, operación de equipos y seguridad de la información, para que las personas no instalen software innecesario y operen bien los equipos, debe instalar software especializado para detectar accesos no autorizados al sistema y así proteger la política de la información confidencial e importante.

Instalaciones.

Se realizó una evaluación a todas las instalaciones del Cabildo y se encontró algunos fallos de seguridad en las instalaciones debido al poco recurso para obtener un espacio adecuado en la organización y la confianza que se genera ya que hasta ahora no se ha presentado un incidente de seguridad.

Las instalaciones del Cabildo de Corinto no son las más adecuadas, pero cumplen con el objetivo de brindar la atención a los comuneros quienes requieren nuestra ayuda y orientarlos de acuerdo a nuestros conocimientos y responsabilidades que ellos nos han delegado.

Recomendaciones: todos los trabajadores comunitarios del cabildo y, cuando se considere oportuno, los usuarios externos y los terceros que desempeñen funciones dentro de la organización, recibir una adecuada capacitación y actualización periódica en materia de la política, normas y procedimientos. Esto comprende los requisitos de seguridad y las responsabilidades legales, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información, el uso correcto de los recursos en general; como por ejemplo su estación de trabajo y del mantenimiento de los equipos de cómputo utilizados. Para así llevar un buen control en las políticas de seguridad de la información.

Se debe hacer una gestión por parte del represente legal con ayuda de la diferentes ya´jas y orientación de la comunidad para afiliarse a una compañía de seguridad para salvaguardar la integridad de la organización y sus trabajadores comunitarios como también debe crear políticas de ingreso a oficinas, ya´jas y a las instalaciones.

La máxima autoridad (ASAMBLEA) debe crear políticas de ingreso a las instalaciones manejando unas bitácoras de acceso para personas fuera de la organización, asegurar los equipos, realizar un mantenimiento a la infraestructura y certificarse con normas de calidad.

19. **Conclusiones**

En una organización indígena en donde este administrando múltiples información, los procesos, sistemas y redes son activos muy importantes. Definir, lograr, mantener y mejorar la seguridad de la información es esencial para la operación de las actividades y proyecciones que se tiene para toda nuestra comunidad que hace parte de nuestro Resguardo.

Actualmente el Cabildo Indígena, sus sistemas e información enfrentan amenazas de seguridad por eso es importante implementar políticas de seguridad de la información para evitar y reducir los riesgos relevantes como son la perdida y manejo inadecuado de la información. Al implementar COBIT e ISO/IEC 27000 en el Cabildo de Corinto ayudará a mejorar la calidad, fiabilidad y los servicios de TI también se reducirá los riesgos, incidentes, y fallas en los procesos en la perdida de información importante y relevante que obtiene a través del tiempo, en la lucha indígena.

Para conllevar al COBIT e ISO/IEC 27000 en primer lugar se deben ajustar a los requisitos del cabildo indígena de corinto y ser integradas entre sí con los procedimientos internos. COBIT ofrece un marco de control e ISO/IEC 27000 incluye áreas específicas y pueden ser mapeadas en el marco COBIT para así determinar el riesgo en que se encuentra la información.

Además de implementar la metodología MAGERIT se puede realizar un análisis de los riesgos que implica la evaluación del impacto que puede afectar a la seguridad de la información en una organización; Identificando riesgos y amenazas que pueden vulnerar el sistema. La obtención de los resultados de este análisis permite generar recomendaciones que se deben adoptar para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir

su impacto en las políticas de la seguridad de la información de la organización indígena como lo es en este caso el Cabildo Indígena del Resguardo Paéz de Corinto.

INFORME FINAL

Señores:

SA´T WESX y DINAMIZADORES

Autoridades Tradicionales del Cabildo indígena del Resguardo Paéz de Corinto

Una vez finiquitada la auditoria en las instalaciones del Resguardo Paéz de Corinto y partiendo del objetivo de evaluar la seguridad de la información en cuanto a hardware, software e instalaciones, con procesos de auditoría basada en los estándares COBIT e ISO/IEC 27000, con el propósito de establecer recomendaciones, que permitan la definición de políticas, procesos y procedimientos de la organización de la organización indígena con el propósito de auditar la seguridad de la información en las áreas de REPRESENTANTE LEGAL, E´CTXE FXIZA, YA´JA KWE´SX KSXA´WNXI YAT, YA´JA KWE´SX VXIU JXAWSA, YA´JA KWESX KAPIYANXI YAT, evaluando el hardware, software e instalaciones en cada una de estas áreas o YA´JAS.

Se encontraron los siguientes hallazgos positivos:

1. Los trabajadores comunitarios del cabildo indígena del Resguardo Paéz de Corinto se encuentra capacitado para cumplir sus funciones responsablemente.

2. La estructura jerárquica de la organización posee un sistema administrativo bien organizado, en el cual se tiene identificado la importancia de la comunidad y las necesidades que se requieren en nuestro resguardo.

3. Se percibe un ambiente de trabajo éticamente propicio con relación a la administración del personal. El clima laboral es de una colaboración altamente profesional entre todos los trabajadores comunitarios para obtener una buena administración de la organización.

4. La autoridad indígena se encuentra abierta a posibilidades de expansión, proyección y mejoramiento en atención para llegar al wet wet fxizxenxi (ARMONIA) en nuestro gran territorio indígena.

5. La unidad desde la autoridad tradicional y sus trabajadores comunitarios en pro del desarrollo administrativo de la organización es relevante para poder seguir en el proceso enriqueciendo el Plan de Vida del Resguardo de Corinto.

Con la realización de la auditoría se sugiere aplicar las siguientes recomendaciones:

1. Todos los trabajadores comunitarios y cuando se considere oportuno, los pasantes o personal externos y los terceros que desempeñen funciones dentro de la organización, deben recibir una capacitación y orientación por parte de la autoridad y los responsables de cada ya´ja, como también la realización de la política, normas y procedimientos. Esto comprende los requisitos de seguridad y las responsabilidades, así como la capacitación entorno al uso correcto de las instalaciones del procesamiento de información, tanto como la parte de las oficinas e instalaciones de la organización y del mantenimiento de los equipos de cómputo utilizados en cada ya´ja por su respectivo dinamizador.

2. Se debe realizar la verificación de hardware y software para garantizar un óptimo trabajo por parte del trabajador comunitario entorno a su labor para que sea muy eficaz y eficiente en la responsabilidad encomendada.

3. Restringir el acceso a la documentación del sistema al personal externo, pasante para tener seguridad de la información con base a las políticas que maneje el dinamizador encargado del sistema y del equipo de cómputo.

4. La autoridad tradicional debe ordenar la creación de un plan de contingencia para los recursos TI, además de nombrar un jefe de sistemas el cual deberá elaborar un plan.

5. La organización indígena de Corinto debe afiliarse a una compañía de seguridad para salvaguardar la integridad del cabildo y sus dinamizadores comunitarios, como también debe crear políticas de ingreso a oficinas y a instalaciones que manejen información que sea restringida.

6. El dinamizador quién entre a administrar recursos TI debe realizar un mantenimiento preventivo a recursos TI, para asegurar que estos funcionen correctamente y no presenten fallos a la hora del uso, además, debe asegurar la información instalando software especializado para prevenir spyware, ataques informático y malware en los equipos de cómputo.

7. El dinamizador o jefe de sistemas quien delegue la autoridad tradicional del cabildo indígena Paéz de Corinto debe aislar el cableado estructurado para que cuente con alguna protección y que cumpla con estándares de calidad y seguridad, debe crear políticas para la administración de computadores, debe administrar los puertos de acceso, para que el sistema no se vulnere fácilmente, debe limitar la conexión al sistema para que no todas las personas puedan entrar a él.

8. El trabajador comunitario o un equipo de trabajo debe crear políticas de instalación de software y operación de equipos, para que los dinamizadores no instalen software innecesario y

operen bien los equipos, debe instalar software especializado para detectar accesos no autorizados al sistema.

En atención a la auditoría realizada por los estudiantes Billy Kennedy Atillo Campo y Santiago Iles, concluimos que el Cabildo Indígena del Resguardo Paéz de Corinto en concertación al análisis y evaluación de riegos de activos de información tiene un riesgo actual en una escala tolerable y una estimación del impacto moderada, esto quiere decir que la seguridad de la información tiene un nivel de confidencialidad de uso interno, un nivel de integridad normal y un nivel de disponibilidad media ya que nos manifiestan algunos dinamizadores y autoridad tradicional en tener la MALICIA INDIGENA en cada situación entorno al manejo de las políticas de la seguridad de la información.

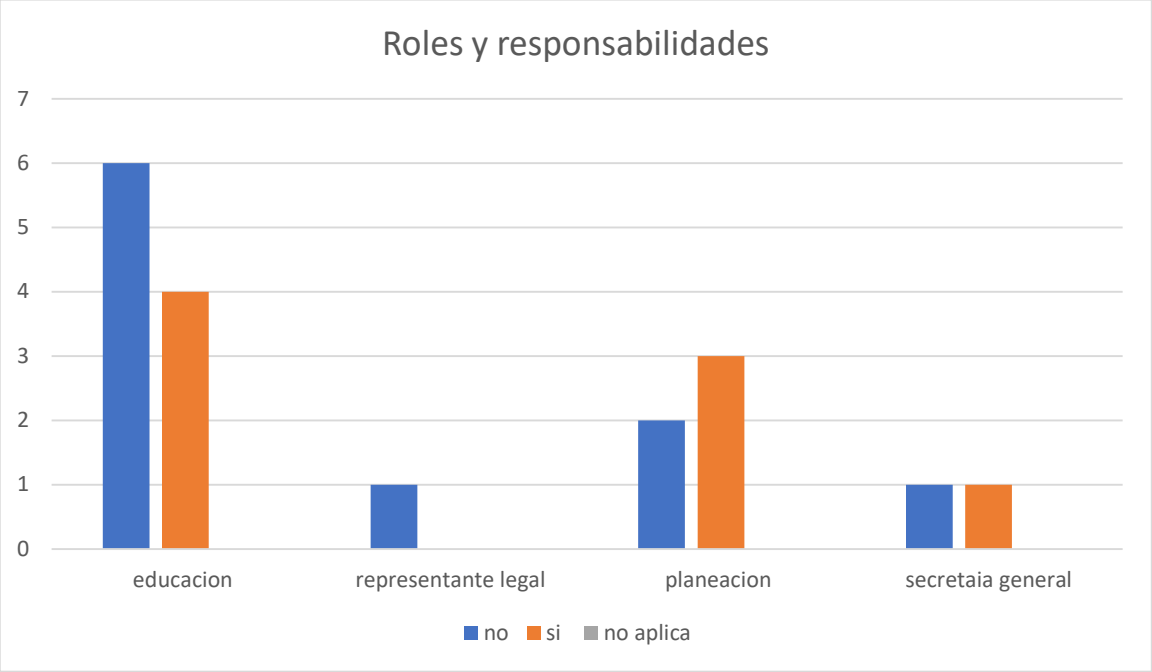
Ilustración 21. Roles y Responsabilidades.

Cuadro 5. Lista de chequeo ROLES Y RESPONSABILIDADES.

CABILDO INDIGENA DEL RESGUARDO PAEZ DE CORINTO					
Dominio	**Planear y Organizar**				
Proceso	**PO4 Definir procesos, organización y relaciones de TI**				
Objetivo de Control	PO4.6 Establecimiento de Roles y Responsabilidades Es necesario establecer un manual de funciones donde se especifiquen los roles y responsabilidades a un dinamizados frente al TI dentro de la organización indígena.				
Cuestionario					
Pregunta		**SI**	**NO**	**N/A**	**OBSERVACIONES**
¿Cuenta la institución con manual de Funciones?			X		
¿Se establecen los roles y responsabilidades de TI?		X			
¿Conoce la organización indígena las Funciones en TI?			X		
¿Hay separación de deberes dentro de la organización?		X			

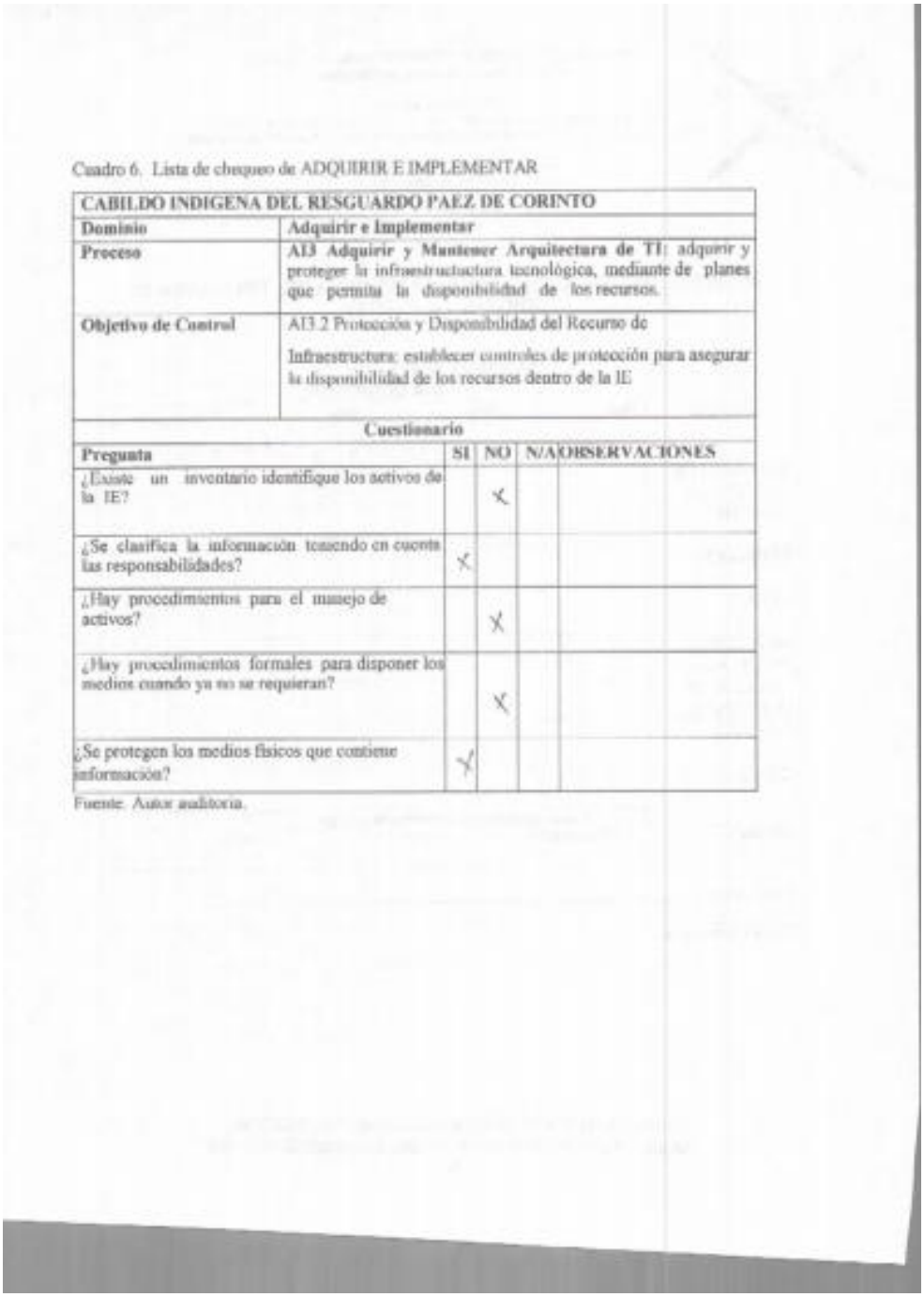
Fuente. Autor auditoria

Fuente. Autor auditoria.



Fuente: Autor Auditoria

Ilustración 22. Adquirir e Implementar



Cuadro 6. Lista de chequeo de ADQUIRIR E IMPLEMENTAR

CABILDO INDIGENA DEL RESGUARDO PAEZ DE CORINTO					
Dominio	**Adquirir e Implementar**				
Proceso	**AI3 Adquirir y Mantener Arquitectura de TI**: adquirir y proteger la infraestructuctura tecnológica, mediante de planes que permita la disponibilidad de los recursos.				
Objetivo de Control	AI3.2 Protección y Disponibilidad del Recurso de Infraestructura: establecer controles de protección para asegurar la disponibilidad de los recursos dentro de la IE				
Cuestionario					
Pregunta		**SI**	**NO**	**N/A**	**OBSERVACIONES**
¿Existe un inventario identifique los activos de la IE?			X		
¿Se clasifica la información tomando en cuenta las responsabilidades?		X			
¿Hay procedimientos para el manejo de activos?			X		
¿Hay procedimientos formales para disponer los medios cuando ya no se requieran?			X		
¿Se protegen los medios físicos que contiene información?		X			

Fuente. Autor auditoria.

Fuente. Autor auditoria.

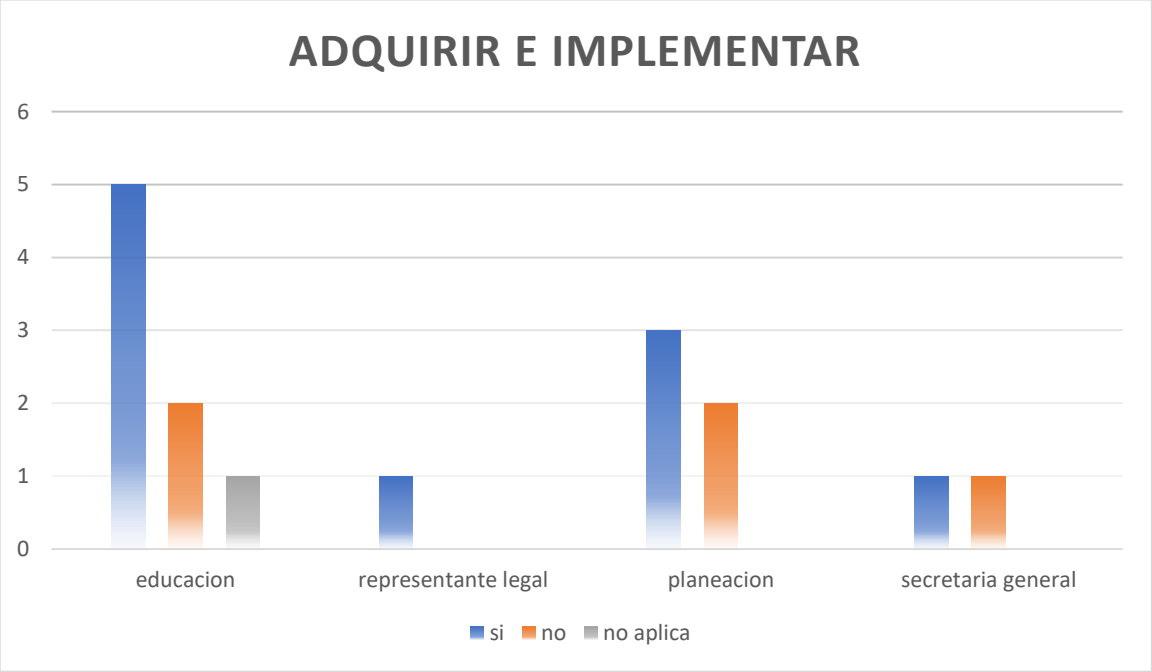
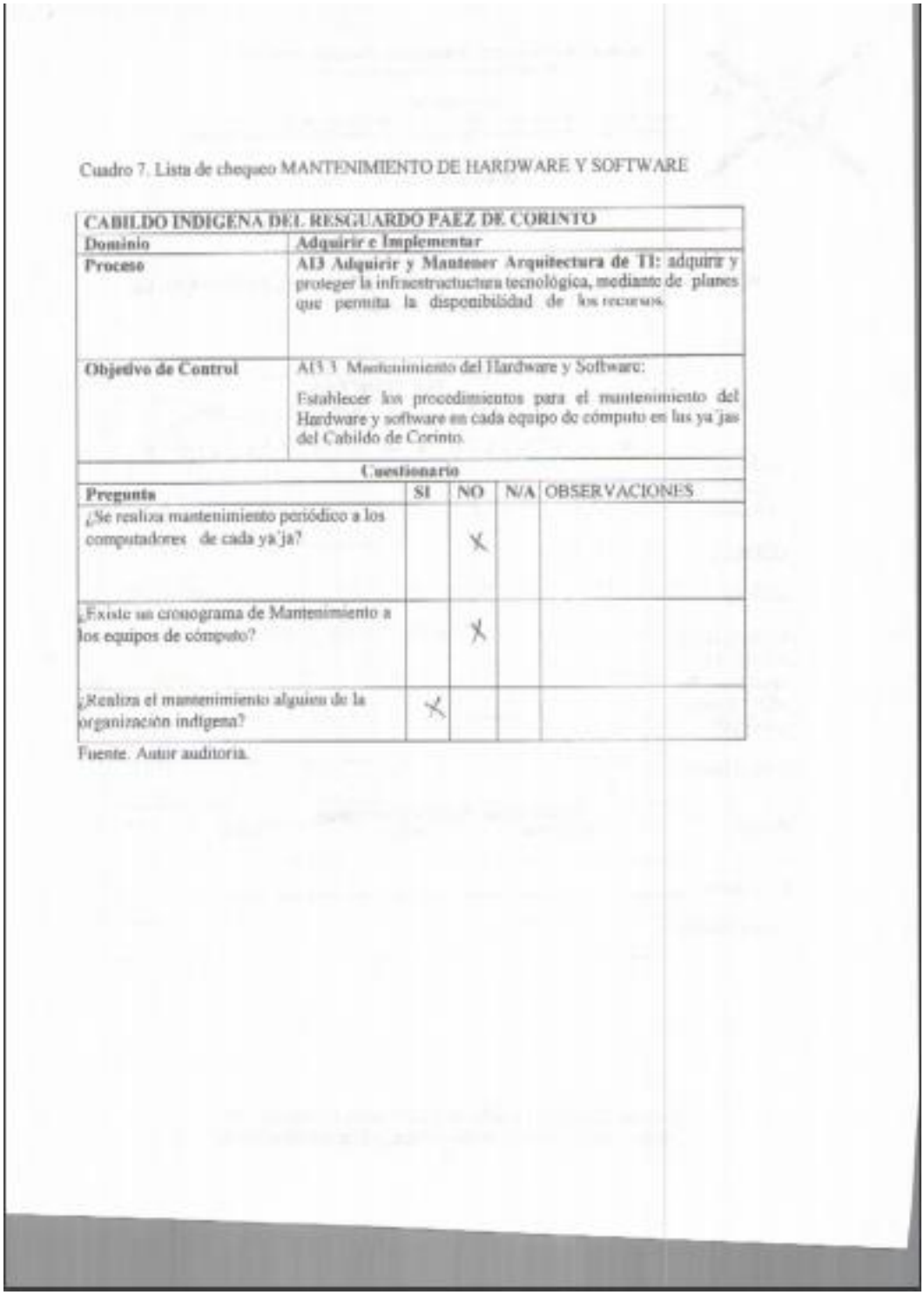

ADQUIRIR E IMPLEMENTAR
6
5
4
3
2
1
0
educacion
representante legal
planeacion
secretaria general
si
no
no aplica

Ilustración 23. . Mantenimiento de Hardware y Software



Cuadro 7. Lista de chequeo MANTENIMIENTO DE HARDWARE Y SOFTWARE

CABILDO INDIGENA DEL RESGUARDO PAEZ DE CORINTO				
Dominio	**Adquirir e Implementar**			
Proceso	**AI3 Adquirir y Mantener Arquitectura de TI:** adquirir y proteger la infraestructuctura tecnológica, mediante de planes que permita la disponibilidad de los recursos.			
Objetivo de Control	AI3 3 Mantenimiento del Hardware y Software: Establecer los procedimientos para el mantenimiento del Hardware y software en cada equipo de cómputo en las ya´jas del Cabildo de Corinto.			
Cuestionario				
Pregunta	**SI**	**NO**	**N/A**	OBSERVACIONES
¿Se realiza mantenimiento periódico a los computadores de cada ya´ja?		X		
¿Existe un cronograma de Mantenimiento a los equipos de cómputo?		X		
¿Realiza el mantenimiento alguien de la organización indígena?	X			

Fuente. Autor auditoria.

Fuente. Autor auditoria.

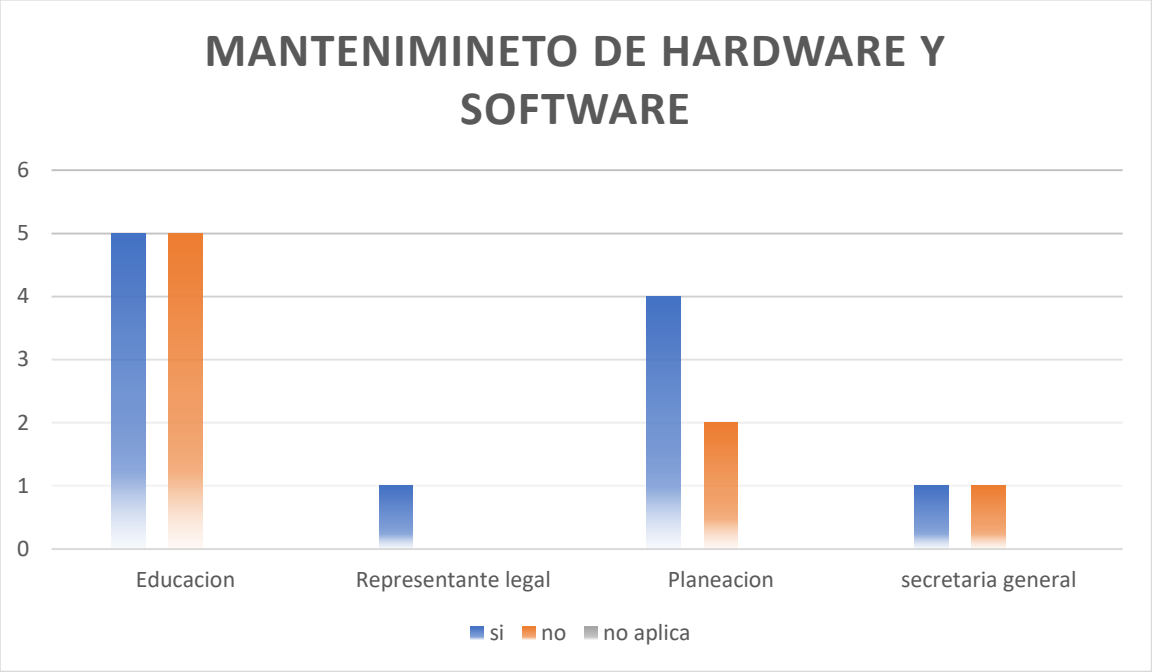
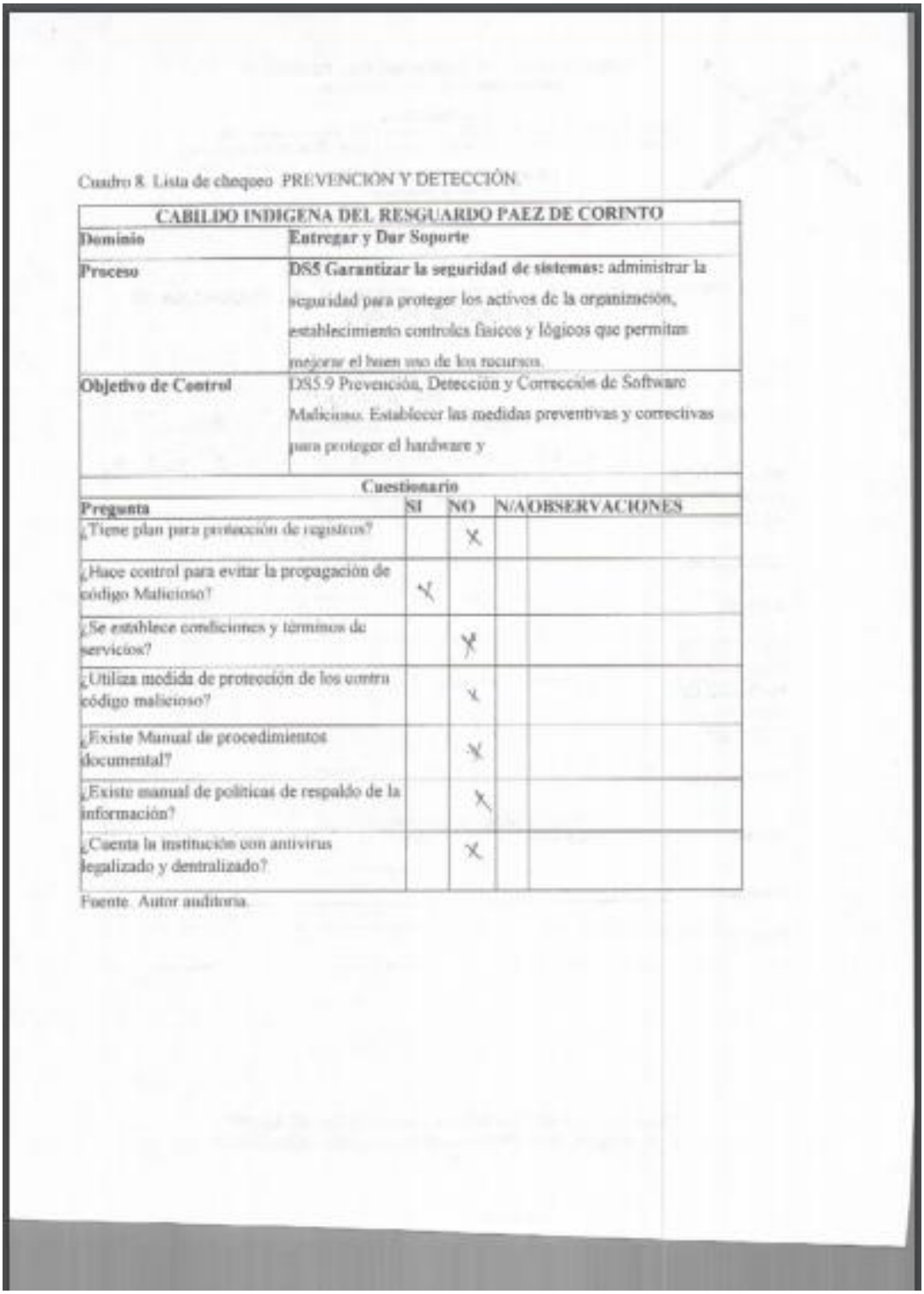

MANTENIMINETO DE HARDWARE Y SOFTWARE
6
5
4
3
2
1
0
Educacion
Representante legal
Planeacion
secretaria general
si
no
no aplica

Ilustración 24. Prevención y Detección.

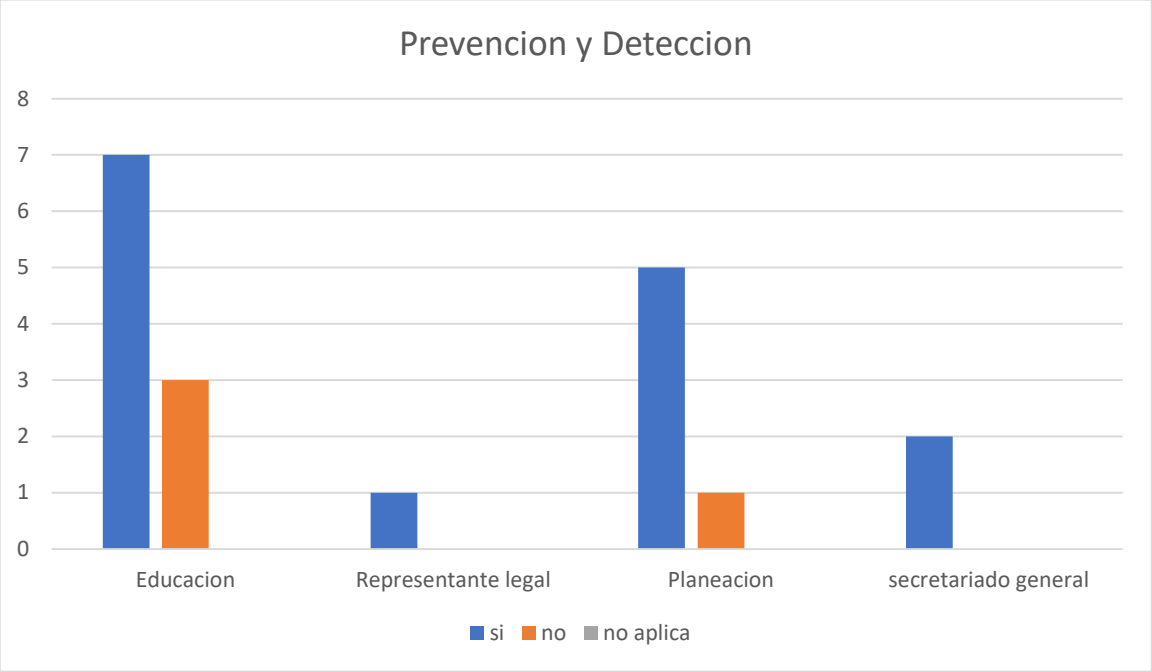


Cuadro 8. Lista de chequeo PREVENCION Y DETECCIÓN.

CABILDO INDIGENA DEL RESGUARDO PAEZ DE CORINTO				
Dominio	**Entregar y Dar Soporte**			
Proceso	**DS5 Garantizar la seguridad de sistemas:** administrar la seguridad para proteger los activos de la organización, establecimiento controles físicos y lógicos que permitan mejorar el buen uso de los recursos.			
Objetivo de Control	DS5.9 Prevención, Detección y Corrección de Software Malicioso. Establecer las medidas preventivas y correctivas para protegr el hardware y			
Cuestionario				
Pregunta	**SI**	**NO**	**N/A**	**OBSERVACIONES**
¿Tiene plan para protección de registros?		X		
¿Hace control para evitar la propagación de código Malicioso?	X			
¿Se establece condiciones y términos de servicios?		X		
¿Utiliza medida de protección de los contra código malicioso?		X		
¿Existe Manual de procedimientos documental?		X		
¿Existe manual de políticas de respaldo de la información?		X		
¿Cuenta la institución con antivirus legalizado y dentralizado?		X		

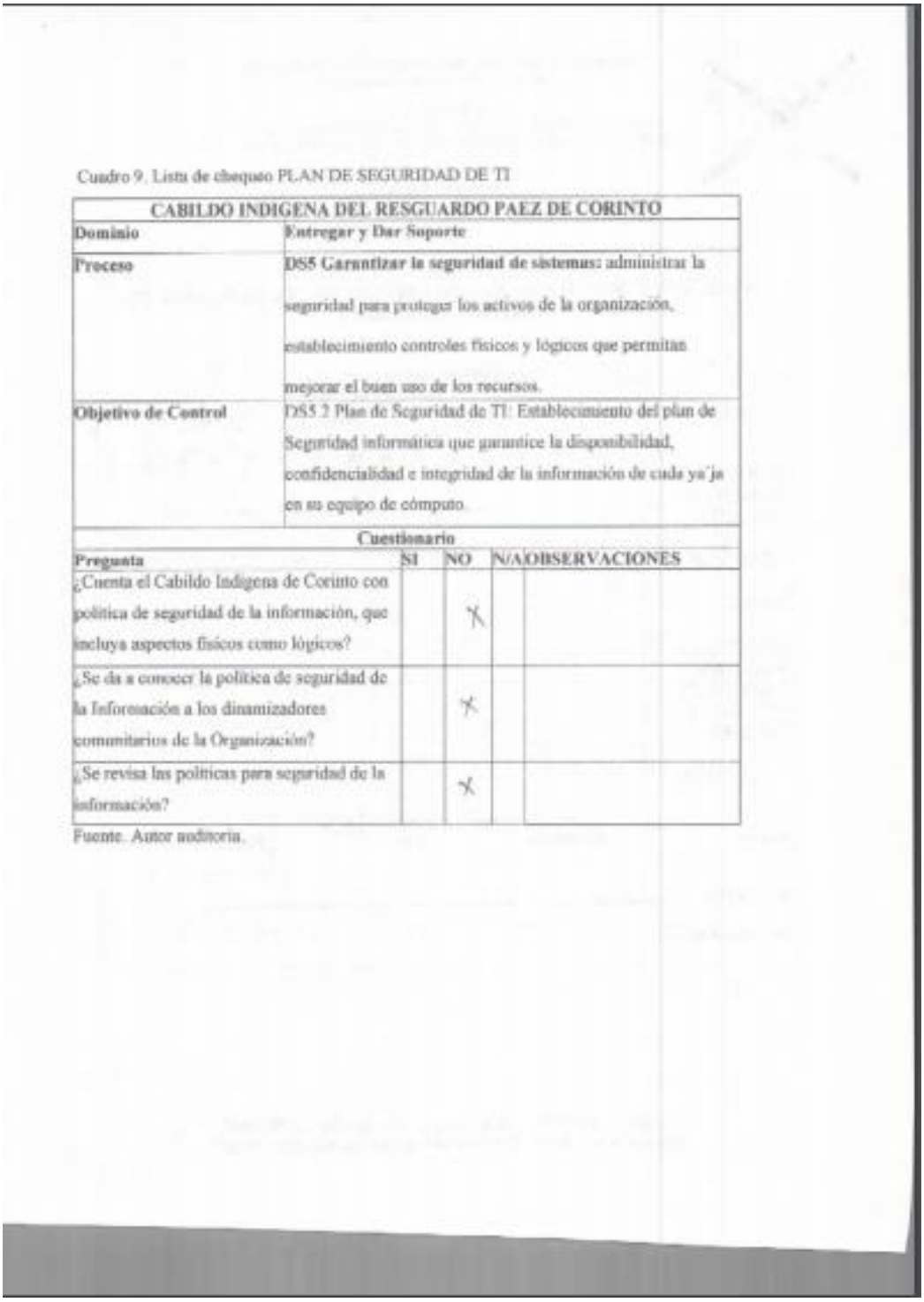
Fuente. Autor auditoria.

Fuente. Autor auditoria.



Fuente. Autor auditoria.

Ilustración 25. Plan de Seguridad de TI.

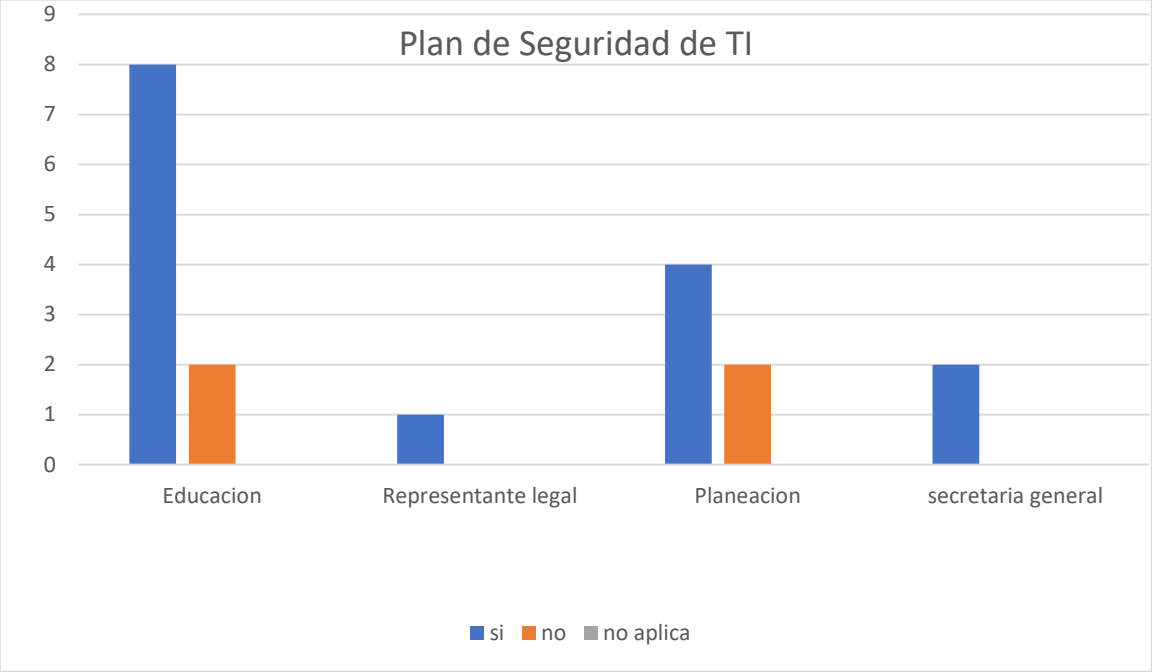


Cuadro 9. Lista de chequeo PLAN DE SEGURIDAD DE TI

CABILDO INDIGENA DEL RESGUARDO PAEZ DE CORINTO				
Dominio	**Entregar y Dar Soporte**			
Proceso	**DS5 Garantizar la seguridad de sistemas:** administrar la seguridad para proteger los activos de la organización, establecimiento controles físicos y lógicos que permitan mejorar el buen uso de los recursos.			
Objetivo de Control	DS5.2 Plan de Seguridad de TI: Establecimiento del plan de Seguridad informática que garantice la disponibilidad, confidencialidad e integridad de la información de cada ya´ja en su equipo de cómputo.			
Cuestionario				
Pregunta	**SI**	**NO**	**N/A**	**OBSERVACIONES**
¿Cuenta el Cabildo Indigena de Corinto con política de seguridad de la información, que incluya aspectos físicos como lógicos?		X		
¿Se da a conocer la política de seguridad de la Información a los dinamizadores comunitarios de la Organización?		X		
¿Se revisa las políticas para seguridad de la información?		X		

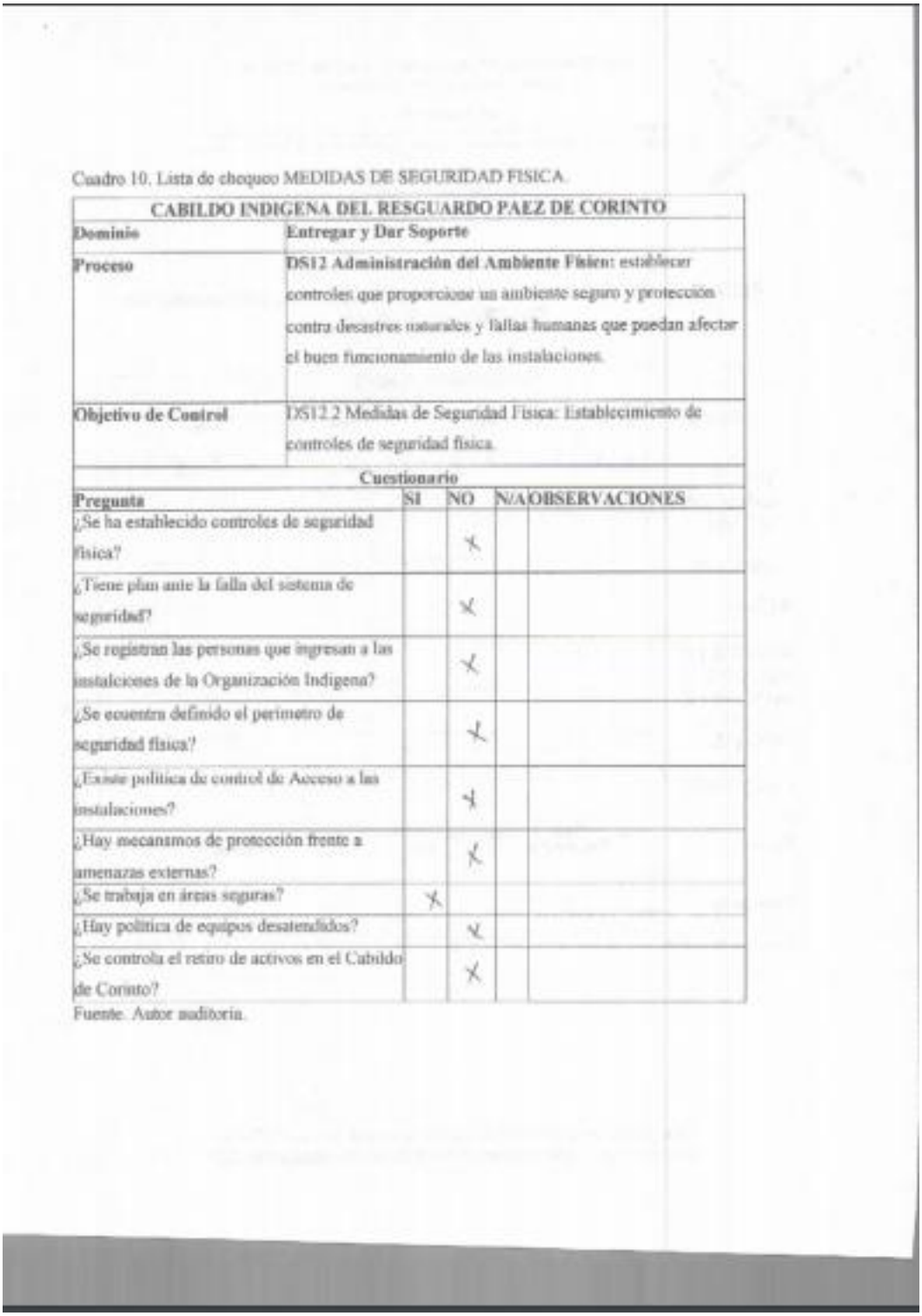
Fuente. Autor auditoria.

Fuente. Autor auditoria.



Fuente: Autor Auditoria

Ilustración 26. *Medidas de Seguridad Física*

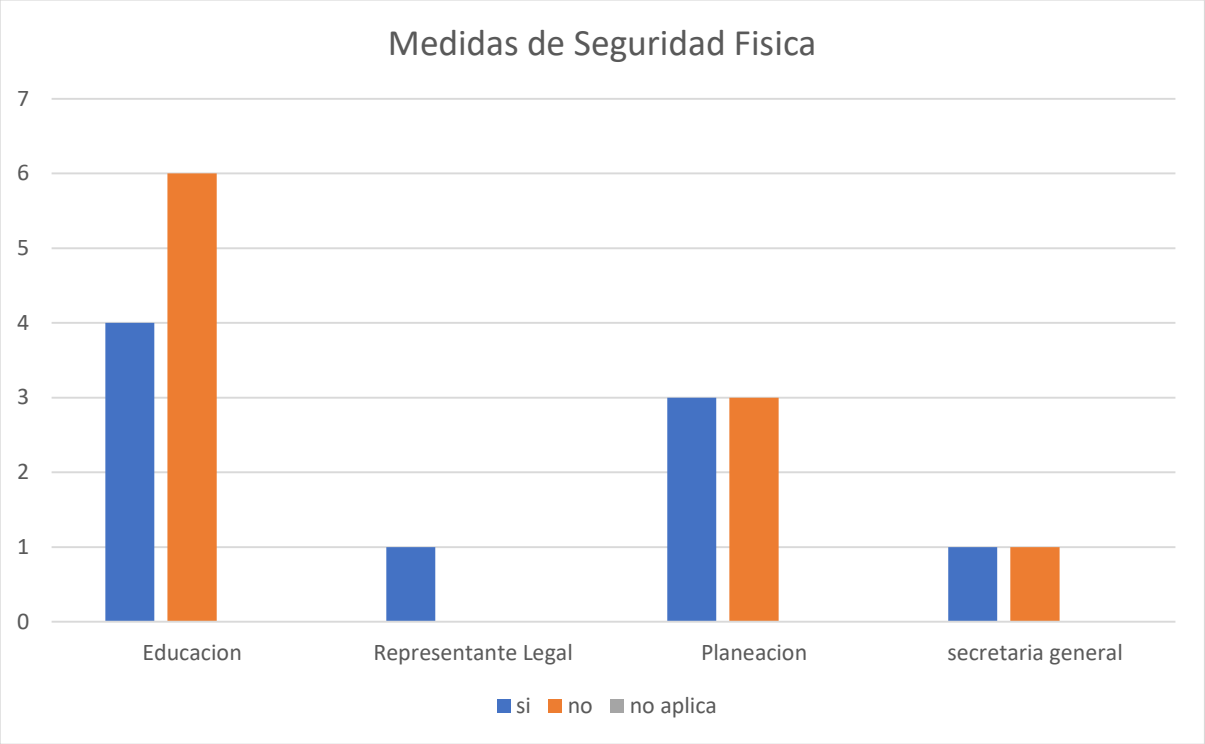


Cuadro 10. Lista de chequeo MEDIDAS DE SEGURIDAD FISICA.

CABILDO INDIGENA DEL RESGUARDO PAEZ DE CORINTO				
Dominio	**Entregar y Dar Soporte**			
Proceso	**DS12 Administración del Ambiente Físico:** establecer controles que proporcione un ambiente seguro y protección contra desastres naturales y fallas humanas que puedan afectar el buen funcionamiento de las instalaciones.			
Objetivo de Control	DS12.2 Medidas de Seguridad Física: Establecimiento de controles de seguridad física.			
Cuestionario				
Pregunta	**SI**	**NO**	**N/A**	**OBSERVACIONES**
¿Se ha establecido controles de seguridad física?		X		
¿Tiene plan ante la falla del sistema de seguridad?		X		
¿Se registran las personas que ingresan a las instalciones de la Organización Indigena?		X		
¿Se ecuentra definido el perimetro de seguridad física?		X		
¿Existe politica de control de Acceso a las instalaciones?		X		
¿Hay mecanismos de protección frente a amenazas externas?		X		
¿Se trabaja en áreas seguras?	X			
¿Hay politica de equipos desatendidos?		X		
¿Se controla el retiro de activos en el Cabildo de Corinto?		X		

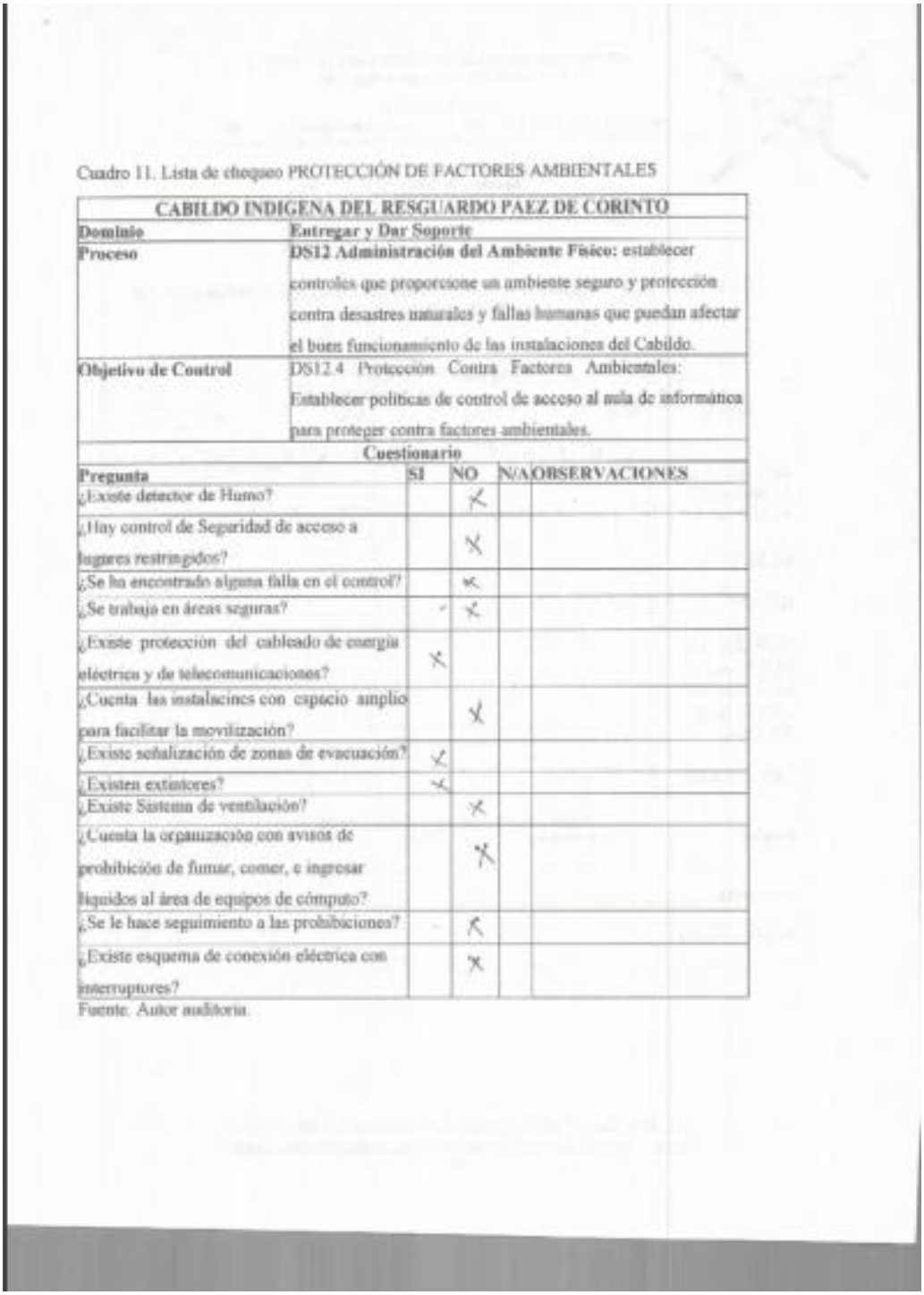
Fuente. Autor auditoria.

Fuente. Autor Auditoria.



Fuente: Autor Auditoria

Ilustración 27. Protección de Factores Ambientales

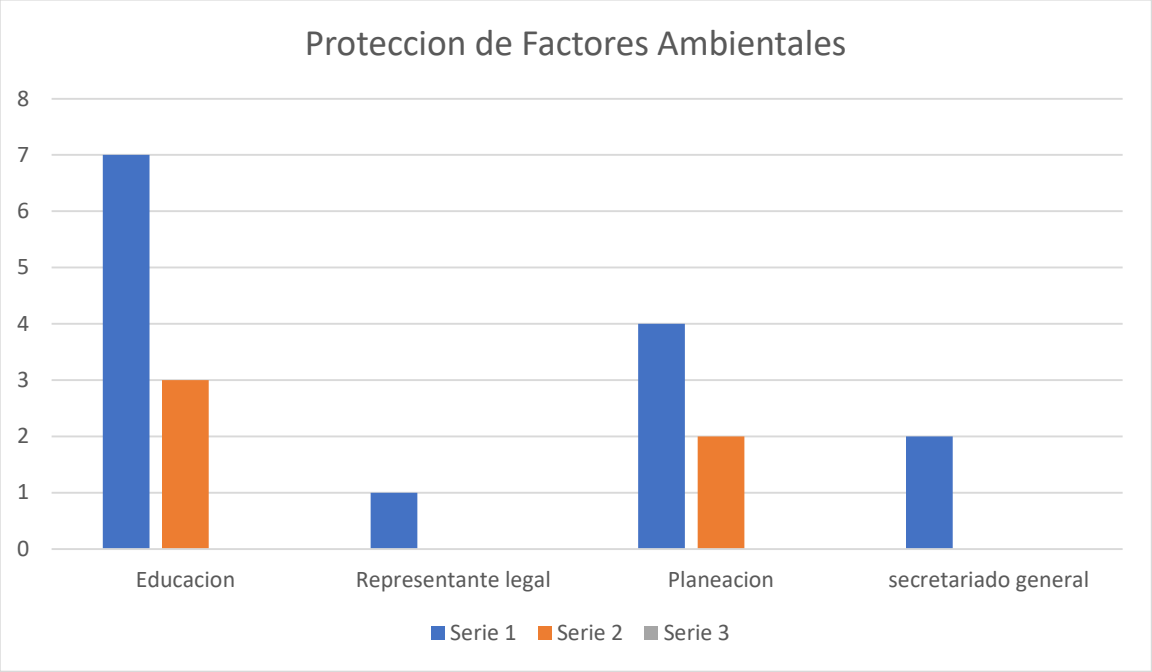


Cuadro 11. Lista de chequeo PROTECCIÓN DE FACTORES AMBIENTALES

CABILDO INDIGENA DEL RESGUARDO PAEZ DE CORINTO				
Dominio	**Entregar y Dar Soporte**			
Proceso	**DS12 Administración del Ambiente Físico:** establecer controles que proporcione un ambiente seguro y protección contra desastres naturales y fallas humanas que puedan afectar el buen funcionamiento de las instalaciones del Cabildo.			
Objetivo de Control	DS12.4 Protección Contra Factores Ambientales: Establecer políticas de control de acceso al aula de informática para proteger contra factores ambientales.			
Cuestionario				
Pregunta	**SI**	**NO**	**N/A**	**OBSERVACIONES**
¿Existe detector de Humo?		X		
¿Hay control de Seguridad de acceso a lugares restringidos?		X		
¿Se ha encontrado alguna falla en el control?		X		
¿Se trabaja en áreas seguras?		X		
¿Existe protección del cableado de energía eléctrica y de telecomunicaciones?	X			
¿Cuenta las instalacines con capacio amplio para facilitar la movilización?		X		
¿Existe señalización de zonas de evacuación?	X			
¿Existen extintores?	X			
¿Existe Sistema de ventilación?		X		
¿Cuenta la organización con avisos de prohibición de fumar, comer, o ingresar liquidos al área de equipos de cómputo?		X		
¿Se le hace seguimiento a las prohibiciones?		X		
¿Existe esquema de conexión eléctrica con interruptores?		X		

Fuente. Autor auditoria.

Fuente. Autor auditorio.



Fuente: Autor Auditoria

Cronograma de actividades.

Actividades	Febrero				Marzo				Abril				Mayo			
	1	2	3	3	1	2	3	4	1	2	3	4	1	2	3	4
Planificación y Organisacion	X	X	X	X	X	X										
Ejecución de la Auditoria					X	X	X	X	X	X						
Consolidacion del Informe Final									X	X	X	X	X	X		

BIBLIOGRAFIA

http://es.wikipedia.org/wiki/Auditor%C3%ADa_de_seguridad_de_sistemas_de_informaci%C3%B3n

http://www.iso27000.es/iso27000.html

Disponible en internet: < URL: http://cs.uns.edu.ar/~ece/auditoria/cobiT4.1spanish.pdf>

Disponible en internet: < URL: http://www.isaca.org/COBIT/Pages/COBIT-5- spanish.aspx

<URL:http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_ Metodolog/ p ae_Magerit.html#.VsZ4EbbhDIU>

URL: http://www.monografias.com/trabajos/auditoinfo/auditoinfo.shtml.>

http://www.iso27000.es/iso27000.html. [Citado enero de 2014].

MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I - Método. [En línea] Disponible en internet. https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/Libro_I_ metodo.pdf. [Citado Julio de 2014]:

http://es.wikipedia.org/wiki/Auditor%C3%ADa_de_seguridad_de_sistemas_de_informaci%C3%B3n

http://www.iso27000.es/iso27000.html

ISACA. Cobit 4.1. [En Línea]. 2007. [Citado el 1 de diciembre de 2015]. Disponible

Disponible en internet: < URL: http://cs.uns.edu.ar/~ece/auditoria/cobiT4.1spanish.pdf>

ISACA. Cobit 5 Introduccion. [En Línea]. 2007. [Citado el 1 de diciembre de 2017]. Disponible Disponible en internet: < URL: http://www.isaca.org/COBIT/Pages/COBIT-5-spanish.aspx>

KIM & SOLOMON, David, Michael G, Fundamentals of information systems security, Jones and Bartlett learning, 1st edition, 2010.

GOBIERNO DE ESPAÑA. MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I [En línea] [Citado el: 15 de 09 de 2015.]. Disponible en internet: <URL:http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_ Metodolog/ p ae_Magerit.html#.VsZ4EbbhDIU>

Auditoría Informática. [En línea] [Citado el: 03 de 10 de 2015.] Disponible en internet: < URL: http://www.monografias.com/trabajos/auditoinfo/auditoinfo.shtml.>

EL PORTAL DE ISO 27001 EN ESPAÑOL. [En línea] Disponible en internet. http://www.iso27000.es/iso27000.html. [Citado enero de 2014].

MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I - Método. [En línea] Disponible en internet. https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/Libro_I_ metodo.pdf. [Citado Julio de 2014].