DISEÑO DE UN SISTEMA DE SEGURIDAD DE PREVENCIÓN Y GESTION DE RIESGO PARA EL INSTITUTO DE INVESTIGACIONES AMBIENTALES DEL PACIFICO JHON VON NEUMANN QUE MINIMICE LOS ATAQUES CIBERNÉTICOS Y ASEGURE LOS ACTIVOS DE INFORMACIÓN A PARTIR DE LA NORMA ISO 27001

LIBIA YISSETH PAZ LAGAREJO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
QUIBDO
2023

DISEÑO DE UN SISTEMA DE SEGURIDAD DE PREVENCIÓN Y GESTION DE RIESGO PARA EL INSTITUTO DE INVESTIGACIONES AMBIENTALES DEL PACIFICO JHON VON NEUMANN QUE MINIMICE LOS ATAQUES CIBERNÉTICOS Y ASEGURE LOS ACTIVOS DE INFORMACIÓN A PARTIR DE LA NORMA ISO 27001.

LIBIA YISSETH PAZ LAGAREJO

Proyecto de Grado – Monografía presentado para optar por el título de ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Danny Fernando León Jaramillo
Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
QUIBDO
2023

NOTA DE ACEPTACIÓN

Firma del presidente de Jurado

Firma del Jurado

Firma del Jurado

Quibdó, 09, 02, 2023

DEDICATORIA

Con amor y cariño dedico ese proyecto a Dios quien ha sido mi fuerza, mi bastón mi ancla en todo este proceso, a mi esposo, padres, hermano y demás familiares por colaborar en todo momento, por apoyarme, darme consejos y por su paciencia. Al director y coordinador de sistemas del Instituto de Investigaciones Ambientales del Pacifico por la oportunidad de aceptar que el proyecto de grado sea aplicado en la institución. Al personal educativo de la Universidad Nacional Abierta y a Distancia en especial al director de proyecto por su paciencia, compañía, correcciones y enseñanzas.

AGRADECIMIENTOS

Agradezco a las directivas de la Universidad Nacional Abierta y a Distancia UNAD, quienes con su trabajo continuo nos brindan la oportunidad de estudiar y laborar, por otro lado, a cada uno de los tutores y asesores que me acompañaron en el proceso les reconozco que sin su apoyo y colaboración éste logro no hubiera sido posible.

CONTENIDO

pág.

LISTA DE TABLAS

LISTA DE FIGURAS

LISTA DE ANEXOS

LISTA DE CUADROS

GLOSARIO

ACTIVO: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

ACTIVOS DE INFORMACIÓN. "En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal." [1]

AMENAZA: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

ANÁLISIS DE RIESGO: "Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000)".[2]

CONFIDENCIALIDAD. Información que no está a disipación del público, ni puede ser revelada a terceros. En caso de que se requiera de la información debe firmar un documento de confidencialidad y determinar el objetivo del porque requiere la información.

COPIAS DE SEGURIDAD. La copia de seguridad, también llamada respaldo o backup, se refiere a la copia de archivos físicos o virtuales o bases de datos a un sitio secundario para su preservación en caso de falla del equipo u otra catástrofe.

DATOS. Información o testimonio de un atributo o variable

DISPONIBILIDAD. Propiedad de que la información y sus recursos relacionados deben estar disponibles y utilizables cuando se los requiera.

GESTIÓN DE ACTIVOS. Radica en tener el más alto rendimiento los bienes o recursos de una entidad u organización, es decir, de todo aquello que tenga valor.

GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN: Gestión de incidentes de seguridad de la información. Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

---

[1] Mintc. Modelo de Seguridad y privacidad de la informacion . Obtenido de Seguridad y Privacidad de la Informacion. 2016.

[2] Ibid

INCIDENTE. Un incidente de seguridad de la información se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a una Política de Seguridad de la Información.[3]

INFORMACIÓN. Es un conjunto de datos acerca de algún suceso, hecho, fenómeno o situación, que organizados en un contexto determinado tienen su significado, cuyo propósito puede ser el de reducir la incertidumbre o incrementar el conocimiento acerca de algo.

INFORMÁTICA. procesamiento automático de información mediante dispositivos electrónicos y sistemas computacionales.

INTEGRIDAD. Integrar la información y sus procesos disponibilidad. acceso a la información para hacer uso de esta.

ISO 27001: Norma internacional para el aseguramiento, confidencialidad e integridad de los datos, información o sistemas que la procesan. Permite a las organizaciones o entidades la evaluación del riesgo y aplicaciones de controles para mitigar o eliminarlos.

RIESGO. Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

SALVAGUARDAR. Proteger un bien ya sea físico o electrónico.

SEGURIDAD. Seguridad es un conjunto de sistemas, medios organizativos, medios humanos y acciones dispuestas para eliminar, reducir o controlar los riesgos y amenazas que puedan afectar a una persona a una entidad. La seguridad proporciona las condiciones para afrontar el peligro, en síntesis, seguridad es la minimización del riesgo.

SEGURIDAD DE LA INFORMACIÓN: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SGSI: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos

[3]

de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

SISTEMA OPERATIVO. Un sistema operativo es el software o programa más importante que se ejecuta en un computador, nos permite usarlo y darle órdenes para que haga lo que necesitamos.

SEGURIDAD INFORMÁTICA. Conjunto de herramientas, procedimientos y estrategias que tienen como objetivo garantizar la integridad, disponibilidad y confidencialidad de la información de una entidad en un sistema.

VULNERABILIDAD. Vulnerabilidad es el riesgo que una persona, sistema u objeto puede sufrir frente a peligros inminentes, sean ellos desastres naturales, desigualdades económicas, políticas, sociales o culturales.

RESUMEN

Este proyecto fue desarrollado con el propósito de diseñar un sistema de seguridad de prevención y gestión de riesgo a partir de la norma ISO 27001 para una entidad del sector público, buscando minimizar los ataques cibernéticos y asegurar los activos de información.

Por consiguiente, se desarrollan 4 estrategias para el diseño del sistema de seguridad. Como primero se realiza un inventario de activos de información para determinar los riesgos y fallas a los que están expuestos; Luego, se evaluarán los riesgos de acuerdo con la probabilidad de ocurrencia e impacto utilizando herramientas como encuestas análisis para la detección de amenazas, Lo que permitirá definir los controles y dominios de acuerdo con la norma ISO 27001 para el tratamiento efectivo de riesgos y vulnerabilidades. Por último, establecer políticas de seguridad informática donde se definan responsables, actividades y procesos a seguir.

Palabras Claves: Activos, Ataques cibernéticos, Controles, Dominios, Información, ISO 27001, Seguridad, Vulnerabilidad.

ABSTRACT

This project was developed with the purpose of designing a risk prevention and management security system based on the ISO 27001 standard for a public sector entity, seeking to minimize cyber-attacks and secure information assets.

Therefore, 4 strategies are developed for the design of the security system. As first, an inventory of information assets is carried out to determine the risks and failures to which they are exposed; Then, the risks will be evaluated according to the probability of occurrence and impact using tools such as analysis surveys for the detection of threats, which will allow defining the controls and domains in accordance with the ISO 27001 standard for the effective treatment of risks and vulnerabilities. Finally, establish computer security policies where responsible persons, activities and processes to be followed are defined.

Keywords: Assets, Cyber-attacks, Controls, Domains, Information, ISO 27001, Security, Vulnerability.

INTRODUCCIÓN

"Un sistema de seguridad es la estrategia global que se implementa para proteger los activos y el personal de tu empresa. Por eso, incluye acciones que se llevan a cabo a diario, a corto, mediano y largo plazo."[4]

Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. Los virus informáticos, el "hacking" o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente dentro de la propia organización o aquellos provocados accidentalmente por catástrofes naturales y fallos técnicos.[5]

De acuerdo con lo anterior, y la necesidad de la institución de asegurar su información y demás activos tecnológicos de manera organizada, la ISO plantea como organización internacional de estándares el propósito de un sistema de seguridad de la información para que sean conocidos, minimizado y gestionado los riesgos de seguridad de una forma estructurada, eficiente, y eficaz que se adapta a cambios que se ocasionen los mismos.

Los sistemas de seguridad de prevención y gestión del riesgo son la base esencial en las organizaciones para dar protección adecuada a todos los activos de información que son la materia prima de las mismas. Disminuir, minimizar y mejorar son tres acciones que forman el objetivo por el cual se debe implementar un sistema de seguridad bajo la Normal ISO 270001 que permite a las organizaciones o entidades la evaluación del riesgo y aplicaciones de controles.

El Instituto de Investigaciones Ambientales del Pacifico, sede principal requiere asegurar sus activos de información a partir de la ISO 27001, con el objetivo de minimizar los riesgos que se ven expuestos los activos de información y tecnológicos.

---

[4] Plan de seguridad para tu empresa: 5 elementos indispensables. Disponible en internet: https://comsitec.com.m

[5] ISO/IEC 27001 Sistema de Gestión de Seguridad de la Información. Disponible en internet: https://isocalidadecuador.com/

El presente proyecto aplicado, va encaminado al diseño de un sistema de seguridad de prevención y gestión buscando minimizar los ataques cibernéticos y asegurar los activos de información a partir de la norma ISO 27001. Teniendo como primera base el estado actual de la seguridad de la Institución para así identificar los riesgos a los que se exponen los activos. Para luego evaluar los riesgos de acuerdo con la probabilidad de ocurrencia y al impacto considerando las amenazas y vulnerabilidades y terminar con proponer políticas de seguridad informática con las acciones de gestión, los recursos, responsabilidades y prioridades para manejar los riesgos de seguridad de la información.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

El Instituto de Investigaciones Ambientales del pacifico en el ámbito de seguridad, no cuenta con políticas que respalden la seguridad de la información como activo más importante de la misma.

Desde que fue creada la planta administrativa del Instituto de Investigaciones Ambientales del Pacifico, los activos de información como base de datos, datos financieros, proyectos de investigación, informaciones personales de los usuarios estuvieron sin protección, es decir cualquier miembro interno o externo tendría acceso a la misma. Para el año 2017 se obtiene un software contable dando esta mejora en los tramites financieros.

Los equipos de cómputo, en especial donde reposa información institucional de gran importancia no cuentan con seguridad lógica, es decir, cualquier usuario puede ingresar y manipular la información, no tienen contraseña, ni restricción al descargar y ejecutar programas.

Se realizo una prueba de escaneo de seguridad al sitio web del Instituto de Investigaciones Ambientales del Pacifico con las siguientes herramientas:

- Con la herramienta wappalyzer instalada en el explorar de Google Chrome. “Wappalyzer es una extensión del navegador que descubre las tecnologías utilizadas en los sitios web. Detecta sistemas de administración de contenido, tiendas web, servidores web, marcos de JavaScript, herramientas de análisis y muchos más.” [6]

En resumen, el sitio web tiene apache 2.4.29, sistema operativo Ubuntu con una tipografía de Google Font API que admite archivos de código abierto para su diseño.

por consiguiente y analizar más de fondo las vulnerabilidades del servidor utilizado por la página web del IIAP apache 2.4.29 se encontraron 4 vulnerabilidades
con el análisis de CVI METRI con los siguientes resultados:
Gravedad de vulnerabilidad alta con 8.1 lo que indica que está en riesgo la página
Co unas métricas de impacto en Confidencialidad, integridad y disponibilidad altos.

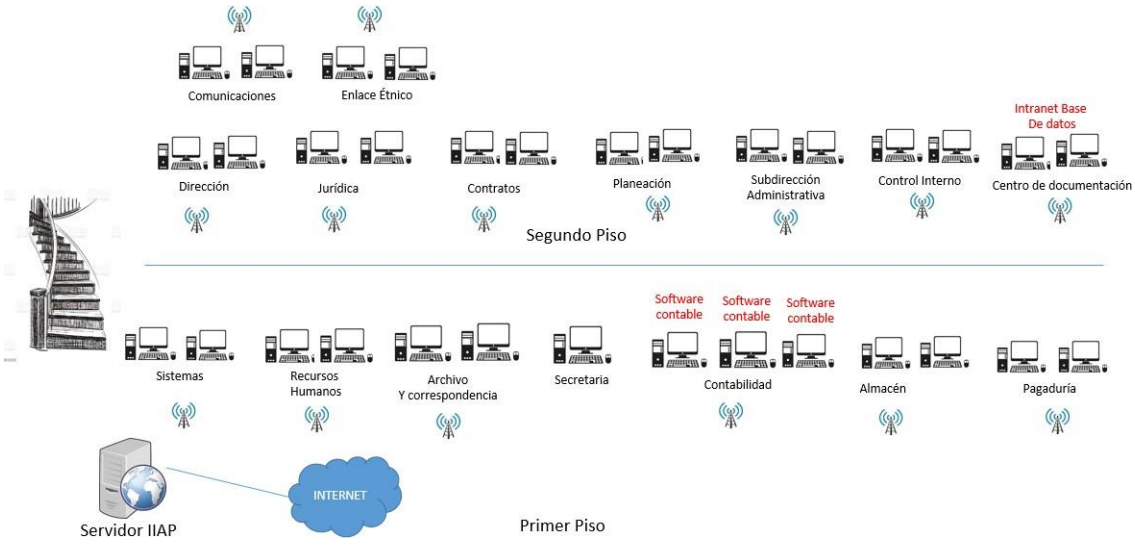
[6] (Wappalyzer - Technology profiler, 2022)

También, se realizó un análisis de vulnerabilidades con la herramienta OWASP ZAP versión 2.11 la herramienta owasp zap es un escáner de seguridad con la intención de realizar pruebas de penetración para comprobar si existen vulnerabilidades. Efectivamente el resultado fueron 10 alertas encontradas en el sitio web del IIAP dos con riesgo alto, dos riesgos medios y el demás riesgo bajo. Lo que indica que si hay riesgo de información en el sitio web y de autenticación.

El Instituto de Investigaciones Ambientales del Pacifico cuenta con un entorno físico de 2 plantas, cuanta con 1 servidor donde se almacena información solamente institucional, una UPC para regular la energía eléctrica y con 30 equipos de cómputo como se muestra en la siguiente imagen:

Distribución entorno físico y tecnológico del Instituto de Investigaciones Ambientales del pacifico sede principal Chocó – Quibdó.

Figura 1.Topología distribución entorno físico y tecnológico. Fuente: Elaboración propia.



no cuenta con señalización de salida de emergencia, ni extintores en caso de incendios.

no cuenta con políticas de seguridad de la información, tampoco con el inventario detallado los activos de información donde se defina la criticidad mediante la disponibilidad, la integridad y confidencialidad.

No cuentan con un documento actualizado donde se definan de roles y responsabilidad para atender casos de incidencias en cuanto a la seguridad, es decir no tiene un directorio activo definido o sistema de gestión de calidad actualizado.

1.2 FORMULACIÓN DEL PROBLEMA

¿Qué acciones, controles y políticas de seguridad se pueden implementar para la gestión de riesgos y la protección de los activos de información del Instituto de investigaciones ambientales del Pacifico John Von Neumann?

2. JUSTIFICACIÓN

Por la naturaleza de la información que manejan las entidades territoriales en sus investigaciones es trascendental contar con un sistema de seguridad que se encargue de proteger su confidencialidad, integridad y disponibilidad. Los sistemas y procesos que manejan esta información se han vuelto necesarios en todas las entidades, pues hacen parte del objetivo misional. Un sistema de seguridad informática se define como una parte fundamental donde las medidas o lineamientos que se establezcan sean de obligatorio cumplimiento para todos los usuarios que utilicen software instalados en la entidad.

Con lo expuesto anteriormente, el diseño de un sistema de seguridad para minimizar los ataques cibernéticos para el Instituto de Investigaciones Ambientales del Pacifico, brinda protección completa al sistema y una mejora a las políticas, gestión del riesgo, personas y procesos.

Para diseñar un sistema de información para la entidad, se realizaron encuestas a los empleados sobre seguridad informática, complementando con un análisis DOFA y/o de brecha.

Con el resultado obtenido de las actividades expuestas anteriormente y con este proyecto se busca construir estrategias para protección de la información mediante controles de seguridad basados en la ISO 27001 y metodologías conocidas que permiten evaluar la seguridad en activos de información. Además, se convierte en una necesidad justa en la cual se pretende indagar, poner en conocimiento y alerta sobre el plan que se debe ejecutar en pro de elevar el nivel de seguridad informática de la entidad.

Por consiguiente, este proyecto beneficia al instituto de investigaciones Ambientales del Pacifico para tener seguridad en la información, trabajar de la mano con el proyecto Gobierno en línea, conocer más de la norma internacional para los sistemas de gestión de la seguridad de la información facilitando la protección de la información.

3. OBJETIVOS

3.1. OBJETIVO GENERAL

- Diseñar un sistema de seguridad de prevención y gestión de riesgos para el Instituto de investigaciones ambientales del Pacifico John Von Neumann buscando minimizar los ataques cibernéticos y asegurar los activos de información a partir de la norma ISO 27001

3.2. OBJETIVOS ESPECÍFICOS

- Determinar los activos de información, los riesgos y las fallas de seguridad presentes en la infraestructura tecnológica y de comunicaciones de la empresa.

- Evaluar los riesgos de acuerdo con la probabilidad de ocurrencia y al impacto considerando las amenazas y vulnerabilidades.

- Definir los controles, procedimientos y estado actual de la entidad para el tratamiento efectivo de los riesgos y vulnerabilidades de acuerdo con la ISO 27001.

- Proponer las políticas de seguridad informática con las acciones de gestión, los recursos, responsabilidades y prioridades para manejar los riesgos de seguridad de la información para el Instituto de investigaciones ambientales del Pacifico John Von Neumann.

4. MARCO REFERNCIAL

4.1. MARCO TEÓRICO

4.1.1. MARCO INSTITUCIONAL.

La ley 99 del 1993 creó el Ministerio del Medio Ambiente, corporaciones autónomas y 5 institutito de investigación científica entre ellos el Instituto de Investigaciones Ambientales del Pacifico John Von Neumann.

Las organizaciones de comunidades negras e indígenas participaron en la creación de este y establecieron lineamientos como visión, misión y objetivos. En su actualidad el director es el Doctor William Klinger Brahan

El instituto de Investigaciones Ambientales del Pacifico tiene como misión desarrollar investigación dirigida a la producción de información y conocimiento del Chocó Biogeográfico que al tiempo que fundamente la toma de decisiones y las políticas públicas nacionales, regionales y locales en materia ambiental y de desarrollo sostenible, promueva el progreso colectivo de los habitantes de la región y consolide la identidad cultural de sus pueblos negros e indígenas, como condiciones necesarias para lograr una paz territorial duradera.

Se visiona en convertirse a 2024 en una institución de investigación referente para el país y el mundo en materia de conocimiento, restauración, manejo y aprovechamiento sostenible del patrimonio natural y cultural del Chocó Biogeográfico, y consecuentemente, en soporte para las decisiones ambientales de los grupos étnicos, autoridades ambientales, gobiernos municipales y departamentales para la planeación del desarrollo territorial y la paz. [7]

Sus principios como institución es el accionar institucional debe basarse en diferentes principios que se constituyan en garantes de una gestión conforme a reglas que generan respeto y reconocimiento social, en este sentido su trabajo debe cubrir la totalidad del territorio de su jurisdicción – territorialidad-, su producción científica y el apoyo a ella debe trascender la frontera de la nación colombiana –

[7] (Pacifico, Instituto de Investigaciones Ambientales del Pacifico, s.f.)

internacionalización -, su dinámica debe procurar la integración de las fuerzas sociales e institucionales de la región – integración –, su ejecución presupuestal y sus resultados deben disponerse a la revisión pública permanente – transparencia -, su manera de hacer las cosas debe garantizar la participación de las comunidades asentadas a lo largo de su territorio – participación – y su accionar deberá conducir a decisiones administrativas y operativas subregionales autónomas – Descentralización

4.1.2. FORTALECIMIENTO TECNOLÓGICO DEL INSTITUTO DE INVESTIGACIONES AMBIENTALES DEL PACIFICO

En el año 2015, los directivos del Instituto elaboraron un diagnóstico para identificar las debilidades que limitaban el buen funcionamiento de las actividades a nivel tecnológico del Instituto. Este diagnóstico arrojo una serie de deficiencias de tipo organizacional y funcional, destacando el atraso tecnológico como una de las principales debilidades.

Con el objetivo de fortalecer el área de sistemas y darle solución a la problemática identificada, el instituto planteó un programa de fortalecimiento tecnológico el cual fue apoyado en abril del 2016 por la junta institucional con las siguientes actividades:

- Apoyo a la actualización y seguridad a los sistemas de Información Institucional.
- Alimentar los distintos sistemas de Información que administra alimenta el IIAP.
- Brindar apoyo en el cumplimiento de los lineamientos del programa GEL.

Los avances o infraestructura tecnológica se considera un apoyo para todas las áreas de la institución, ya que la tecnología es un medio que permite estar en constante avance y actualización.

Por tal razón se estructuró lo siguiente:

- Apoyar el desarrollo y aplicación de nuevas tecnologías que fortalezcan las investigaciones realizadas por el IIAP

- Actualizar los sistemas de información institucional.

- Seguridad y privacidad de la Información

- Garantizar el buen funcionamiento de los equipos y tener el software al máximo rendimiento.

- Todo lo que se ha implementado a nivel tecnológico ha sido soportado informes entregables a la institución.

4.1.3. CIBERSEGURIDAD

Se refiere a la seguridad informática, políticas, procesos, planes y herramientas de hardware y software, con el objetivo de proteger la privacidad, la disponibilidad y la integridad de la información.

Actualmente, los ataques son más avanzados y los atacantes aprovechan toda clase de vulnerabilidad para debilitar los sistemas. Las empresas necesitan soluciones integrales para prevenir, bloquear y remedia los ataques.

4.1.3.1. Contexto Institucional.

El Instituto de Investigaciones Ambientales del Pacifico, no solamente es investigación también, su naturaleza se basa en la parte administrativa donde se realiza todo lo concerniente a contrataciones, contabilidad, bases de datos, datos de investigaciones, pagos de monina, planeación, compras, área TIC, seguridad informática y demás. Es por ello, que los activos de información también son importantes y se deben cuidar.

Además, en apoyo con el ministerio de las TIC están trabajando en el proyecto de Seguridad digital, lo que anteriormente se llamaba gobierno en línea como estrategia a la seguridad informática.

Para el apoyo de todas estas funciones misionales administrativas, el Instituto de Investigaciones Ambientales del Pacifico creó el proyecto de apoyo a la actualización de los sistemas de Información Institucional para alimentar los distintos sistemas de Información que administra y alimenta el IIAP, así como

brindar apoyo en el cumplimiento de los lineamientos del programa Seguridad Digital con el objetivo de estar a la par con la modernización tecnológica y velar por la seguridad de la información.

Razón por la cual se diseña un sistema de seguridad de prevención y gestión de riesgos buscando minimizar los ataques cibernéticos y asegurar los activos de información a partir de la norma ISO 27001 para dar cumplimiento a los objetivos y proyectos de la institución.

4.2. SEGURIDAD INFORMÁTICA

En estos tiempos el uso del internet cada vez va en aumento, así mismo, están es constante comunicación con los socios y proveedores y permiten el acceso a los sistemas de información. Es importante clasificar a que activos o sistema de información del instituto pueden ingresar y controlar el acceso a los mismo.

Integridad. Integrar la información y sus procesos disponibilidad. acceso a la información para hacer uso de la misma.

En términos de seguridad informática la integridad hace referencia la fidelidad de la información previniendo la modificación sin autorización.

Disponibilidad. Propiedad de que la información y sus recursos relacionados deben estar disponibles y utilizables cuando se los requiera.

Referencia a la seguridad informática, la disponibilidad de un activo de información es poder obtener datos siempre y cuando se requiera.

4.3. POLÍTICAS DE SEGURIDAD

Las políticas de seguridad informática son normas y directrices para garantizar la confidencialidad, integridad y disponibilidad de la información y minimizar los riesgos que le afectan. Además, define el conjunto de controles que se deben implementar, procedimientos e instrucciones técnicas que abarca medidas técnicas y organizativas que se establecen para dar cumplimiento a dicha política.

4.4. PLAN DE SEGURIDAD INFORMÁTICA.

Es la expresión gráfica del Sistema de Seguridad Informática diseñado y constituye el documento básico que establece los principios organizativos y funcionales de la actividad de Seguridad Informática en una Entidad y recoge claramente las políticas de seguridad y las responsabilidades de cada uno de los participantes en el proceso informático, así como las medidas y procedimientos que permitan prevenir, detectar y responder a las amenazas que gravitan sobre el mismo.[8]

En el proceso de diseño de un plan de Seguridad Informática se logran identificar 3 etapas.

1. Analizar las necesidades de protección de los activos de información
2. Determinar el plan de seguridad que garantice mitigar los riesgos que fueron identificados.
3. Revisar el plan de seguridad, socializarlo con la alta gerencia y demás empleados de la institución.

4.5. MARCO CONCEPTUAL

ACTIVO: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

ACTIVOS DE INFORMACIÓN: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

AMENAZA: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

[8] Ramirez, J. C. METODOLOGIA PARA LA ELABORACION DEL PLAN DE SEGURIDAD INFORMATICA. Obtenido de plan_seguridad.pdf. 2020.

ANÁLISIS DE RIESGO: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

CONFIDENCIALIDAD: Información que no está a disipación del público, ni puede ser revelada a terceros. En caso de que se requiera de la información debe firmar un documento de confidencialidad y determinar el objetivo del porque requiere la información.

COPIAS DE SEGURIDAD: La copia de seguridad, también llamada respaldo o backup, se refiere a la copia de archivos físicos o virtuales o bases de datos a un sitio secundario para su preservación en caso de falla del equipo u otra catástrofe.

DATOS: Información o testimonio de un atributo o variable

DISPONIBILIDAD: Propiedad de que la información y sus recursos relacionados deben estar disponibles y utilizables cuando se los requiera.

GESTIÓN DE ACTIVOS: Radica en tener el más alto rendimiento los bienes o recursos de una entidad u organización, es decir, de todo aquello que tenga valor.

GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN: Gestión de incidentes de seguridad de la información. Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

INFORMACIÓN: Es un conjunto de datos acerca de algún suceso, hecho, fenómeno o situación, que organizados en un contexto determinado tienen su significado, cuyo propósito puede ser el de reducir la incertidumbre o incrementar el conocimiento acerca de algo.

INFORMÁTICA: procesamiento automático de información mediante dispositivos electrónicos y sistemas computacionales.

INTEGRIDAD: Integrar la información y sus procesos disponibilidad. acceso a la información para hacer uso de la misma.

RIESGO: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

SALVAGUARDAR: Proteger un bien ya sea físico o electrónico.

SEGURIDAD: Seguridad es un conjunto de sistemas, medios organizativos, medios humanos y acciones dispuestas para eliminar, reducir o controlar los riesgos y amenazas que puedan afectar a una persona a una entidad. La seguridad proporciona las condiciones para afrontar el peligro, en síntesis, seguridad es la minimización del riesgo.

SEGURIDAD DE LA INFORMACIÓN: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SGSI: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

SOFTWARE: El software está compuesto por un conjunto de programas que son diseñados para cumplir una determinada función dentro de un sistema, ya sean estos realizados por parte de los usuarios o por las mismas corporaciones dedicadas a la informática.

4.6. MARCO HISTÓRICO

Este capítulo tiene la como objetivo exponer y dar a conocer algunos términos relacionados con este proyecto aplicado, para dar una idea general de los conceptos que están involucrados con la seguridad informática.

Seguridad informática. Durante los años 80 y principios de los 90 la Seguridad Informática se centraba en proteger los equipos de los usuarios, es decir, proporcionar seguridad a los ordenadores y su sistema operativo.

Esta seguridad lógica, entendida como la seguridad de los equipos informáticos para evitar que dejasen de funcionar correctamente, se centraba en la protección contra virus informáticos. Con la aparición de Internet y su uso globalizado a nivel empresarial la Seguridad Informática comenzó a enfocarse hacia la conectividad de redes o networking, protegiendo los equipos servidores de aplicaciones informáticas, y los equipos servidores accesibles públicamente a través de Internet, y controlando la seguridad a nivel periférico a través de dispositivos como Firewalls.[9]

"El pionero en realizar escritos sobre la seguridad informática en el 1980 fue James P. Anderson. Enfocado la seguridad informática como la protección de la infraestructura computacional incluyendo la información contenida." [10]

Principios de la seguridad informática. el objetivo de la seguridad informática es proteger los activos de una organización basado en los siguientes principios: Integridad.

4.7. ANTECEDENTES O ESTADO ACTUAL

4.7.1. ANTECEDENTES.

El Instituto de Investigaciones Ambientales del pacifico en el ámbito de seguridad, no cuenta con políticas que respalden la seguridad de la información como activo más importante de la misma.

Desde que fue creada la planta administrativa del Instituto de Investigaciones Ambientales del Pacifico, los activos de información como base de datos, datos financieros, proyectos de investigación, informaciones personales de los usuarios estuvieron sin protección, es decir cualquier miembro interno o externo tendría acceso a la misma. Para el año 2017 se obtiene un software contable dando esta mejora en los tramite financieros.

Los equipos de cómputo, en especial donde reposa información institucional de gran importancia no cuentan con seguridad lógica, es decir, cualquier usuario puede ingresar y manipular la información, no tienen contraseña, ni restricción al descargar y ejecutar programas.

---

[9] JYCELL-NUMAEL. Seguridad Informática. Historia de la seguridad informática. 2017

[10] Eugene Spafford y James P. Anderson. SECURITY&PRIVACY, Obtenido de James P. Anderson: un pionero en seguridad de la información. p. 9 Vol. 6.

Se realizo una prueba de escaneo de seguridad al sitio web del Instituto de Investigaciones Ambientales del Pacifico con las siguientes herramientas:

- Con la herramienta wappalyzer instalada en el explorar de Google Chrome. “Wappalyzer es una extensión del navegador que descubre las tecnologías utilizadas en los sitios web. Detecta sistemas de administración de contenido, tiendas web, servidores web, marcos de JavaScript, herramientas de análisis y muchos más.” [11]

En resumen, el sitio web tiene apache 2.4.29, sistema operativo Ubuntu con una tipografía de Google Font API que admite archivos de código abierto para su diseño.

por consiguiente y analizar más de fondo las vulnerabilidades del servidor utilizado por la página web del IIAP apache 2.4.29 se encontraron 4 vulnerabilidades con el análisis de CVE MITRE con los siguientes resultados:

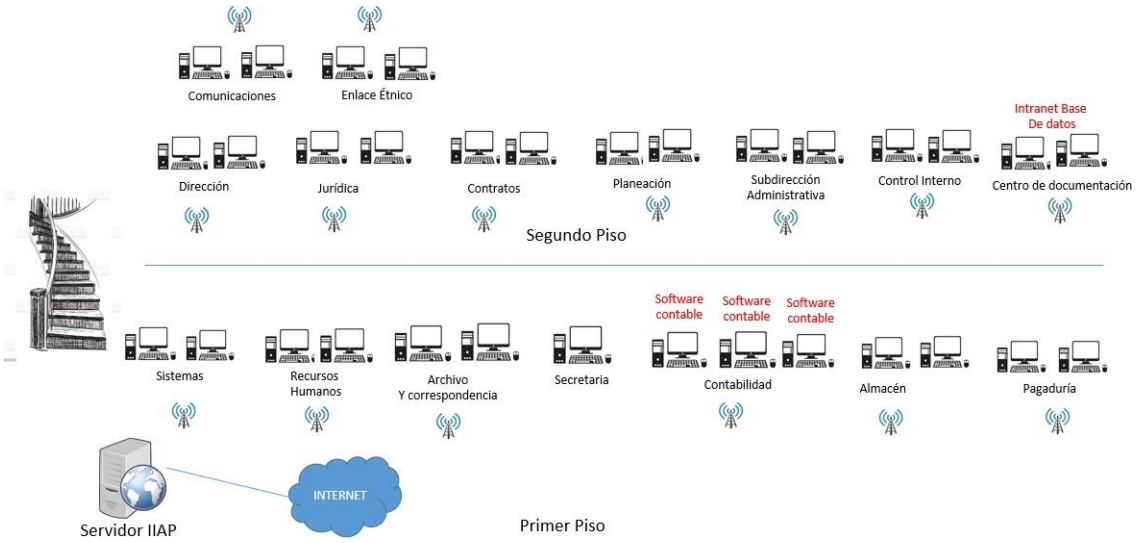
Gravedad de vulnerabilidad alta con 8.1 lo que indica que está en riesgo la página Co unas métricas de impacto en Confidencialidad, integridad y disponibilidad altos. También, se realizó un análisis de vulnerabilidades con la herramienta OWASP ZAP versión 2.11 la herramienta owasp zap es un escáner de seguridad con la intención de realizar pruebas de penetración para comprobar si existen vulnerabilidades. Efectivamente el resultado fueron 10 alertas encontradas en el sitio web del IIAP dos con riesgo alto, dos riesgos medios y el demás riesgo bajo. Lo que indica que si hay riesgo de información en el sitio web y de autenticación.

El Instituto de Investigaciones Ambientales del Pacifico cuenta con un entorno físico de 2 plantas, cuanta con 1 servidor donde se almacena información solamente institucional, una UPC para regular la energía eléctrica y con 30 equipos de cómputo como se muestra en la siguiente imagen:

Distribución entorno físico y tecnológico del Instituto de Investigaciones Ambientales del pacifico sede principal Chocó – Quibdó.

[11] (Wappalyzer - Technology profiler, 2022)

topología distribución física y tecnológica del Instituto de Investigaciones Ambientales del Pacifico (antes de la implementación del proyecto). Fuente: Elaboración propia.



Seguido, el Instituto de Investigaciones Ambientales del Pacifico cuenta con dos sistemas de información donde se almacena toda la información de los proyectos que realiza la misma, se llama centro de documentación y la información contable con el software Helisa.

De acuerdo a la encuesta y análisis de seguridad realizado a todos los empleados, los resultados arrojados dieron un alto riesgo de pérdida de información y ataques de vulnerabilidades, esto se debe a que los equipos no cuentan con ningún proceso de seguridad, No tiene antivirus, los usuarios no han recibido capacitaciones sobre seguridad de la información, el acceso a la base de datos es desde la página web que también presenta vulnerabilidades e impacto de nivel Crítico en confidencialidad, integridad y disponibilidad. la información está expuesta al público lo que también coloca en riesgo todos los proyectos de investigación.

Los usuarios tienen la clave de fácil acceso para terceros lo que implica un abuso de privilegio de acceso y pueden ocurrir vulnerabilidades y es un activo de mayor grado debido al contenido. Para poder obtener información de investigación se debe solicitar al personal encargado, pero teniendo los equipos sin seguridad de inicio cualquier usuario puede acceder a la información sin realizar una solicitud.

En el año 2018 se realizó un diagnóstico en una matriz DOFA sobre la seguridad informática del Instituto con los siguientes resultados.

CUADRO 1. Matriz DOFA para la identificación de riesgos

	MATRIZ DOFA PARA IDENTIFICACIÓN DE RIESGOS		
PROCESO:	**Administrativo**		
OBJETIVO:	Determinar la problemática existente en la organización de acuerdo al diagnóstico realizado que le permita a la organización enfrentar de manera adecuada y oportuna los aspectos cambiantes derivados del análisis interno.		
FECHA:	**11/07/2018**		
DEBILIDADES	**FUENTE**	**AMENAZAS**	**FUENTE**
		Falta antivirus	Falta de presupuesto para comprar la licencia.
Ausencia de un sistema de copias de Seguridad	NA	**Perdida de información institucional**	
Ausencia de Buenas Prácticas.	No hay manual que estipule realizar buenas prácticas, falta de capacitaciones al personal administrativo y técnico		
		Software Helisa	No es un software confiable. Incongruencia en las nóminas. Retraso en los pagos
Equipos de cómputo sin seguridad o protección	Sin protección	Expuesto a ataques y vulnerabilidades Abusos de privilegios	

		Manipulación de información por terceros	
Ausencia de políticas de seguridad		Si hay perdida, robo, daño de equipo no hay políticas que direccionen que hacer en caso de que ocurran las anormalidades anteriores	
Ausencia de un sistema de seguridad para mitigar riesgos		No existe un sistema donde se haya evaluado las posibles amenazas ni como abordarlas en caso de que ocurran.	
Información	Sin respaldo.	No se realiza el adecuado proceso en las copias de seguridad para la información de la entidad	

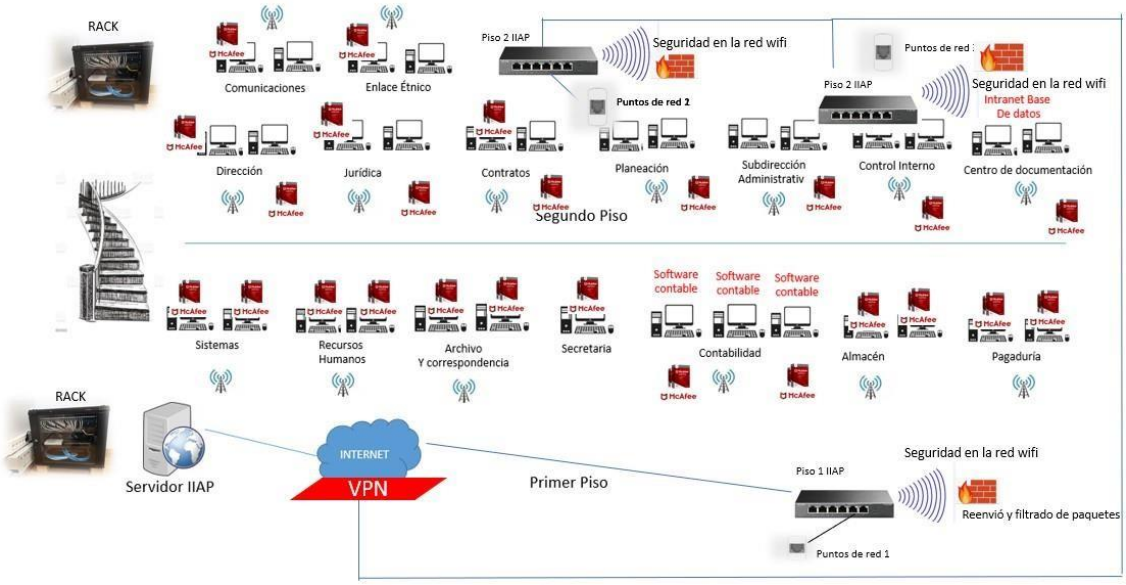
4.7.2. ACTUALIDAD.

Actualmente, El Instituto de Investigaciones Ambientales del Pacifico tiene como misión desarrollar investigación dirigida a la producción de información y conocimiento del Chocó Biogeográfico. Como Instituto tiene 4 sedes, una administrativa en la Ciudad de Quibdó como principal, en Tumaco, vía Yuto – Choco, Bogotá y Buenaventura.

En la sede principal está todo lo relacionado con la parte administrativa con las oficinas de Sistemas, Recursos humanos, Enlace étnico, comunicaciones, contabilidad, pagaduría, almacén, archivo y correspondencia, Contratos, Jurídica, Planeación, Subdirección y Control Interno.

Tecnológicamente tiene una topología de red definida como se muestra en la siguiente figura.

Figura 2.Propuesta topología de red del Instituto de Investigaciones Ambientales del Pacifico. Elaboración: Fuente propia del autor.



Edificio de 2 plantas, cuanta con 1 servidor donde se almacena información solamente institucional, una UPC para regular la energía eléctrica y con 30 equipos de cómputo distribuidos en las áreas mencionadas anteriormente.

Cuenta con políticas de seguridad de recursos tecnológicos. También, con la guía sobre metodología y administración del riesgo, guía de incidentes de la seguridad de la información.

Los equipos para su mejor funcionamiento tienen un plan de mantenimiento preventivo y backup que se realiza cada mes y políticas de respaldo de información donde se estipula todo lo relacionado con la seguridad de la información y la importancia de realizar backup.

Señalización de emergencia, software contable en la nube con proveedores externos, base de datos actualizada para el centro de documentación con seguridad de contraseñas y políticas de gestión de contraseña.

Roles y responsabilidades en incidencias de seguridad de la información, actualidad del sistema de gestión de calidad de la entidad evaluado y revisado por la alta gerencia y jefes de cada área, gestor visor para la creación de mapas para los proyectos de investigaciones.

Proceso de Backup.

- Cronograma de Backup realizado por el equipo TIC y aprobado por el director de la misma área.

- Se le notifica al usuario un día antes el horario que se realizara la copia de seguridad vía correo electrónico y que guarde o elimine toda información personal.

- Selección del material para respaldar. Este proceso se hace el encargado del área TIC y el responsable del equipo.

- Trámite de analizar la importancia de los activos de información que se tiene almacenado en el equipo.

- Se procede a realizar el almacenamiento de la información institucional en el disco Nas (disco local).

- Termina el proceso de backup.

El Instituto de Investigaciones Ambientales del Pacifico, cuenta con un documento seguridad digital, guía y matriz de inventario y clasificación de activos, en construcción para ser revisado por alta gerencia.

Casos de Incidentes de seguridad.

Abuso de privilegios de acceso. El mal manejo de las credenciales para ingresar a la base de datos provoco el desvió de información financiera.

Auto relleno de inicio de sesión. El relleno automático de las credenciales al ingresar al sistema provoco un bloqueo del sistema de información y no se reportó información financiera dos días

Falta de contraseña al inicio. Al no tener seguridad de contraseña al iniciar sección se vio afectada la información de eliminación de algunos datos financieros por alguien que ya no hacia parte de la institución.

En la actualidad esos casos de incidencias de vulnerabilidad han sido tratados porque se tiene plena definición sobre cómo actuar ante cualquier caso de vulnerabilidad, plan de gestión de contraseñas lo que ya no permite que haya abuso de privilegio de acceso.

De acuerdo con lo anterior se presenta los resultados obtenidos de la matriz DOFA:

CUADRO 2. Matriz DOFA para identificación de riesgos actualizada

	MATRIZ DOFA PARA IDENTIFICACIÓN DE RIESGOS		
PROCESO:	**Administrativo**		
OBJETIVO:	Determinar la problemática existente en la organización de acuerdo con el diagnóstico realizado que le permita a la organización enfrentar de manera adecuada y oportuna los aspectos cambiantes derivados del análisis interno.		
FECHA:	**11/24/2022**		
DEBILIDADES	**OPORTUNIDADES**	**FORTALEZAS**	**AMENAZAS**
	Políticas de seguridad de la información	Respuestas ante incidentes de vulnerabilidades en los sistemas.	
	Bitácora de copias de seguridad y plan de procedimiento.	Cuenta con un servidor para realizar copias de seguridad de la información.	
	Sistema de gestión de calidad actualizado.	Cuenta con manual de gestión sistema de Calidad incluyendo las buenas prácticas tanto administrativas como tecnológicas	
	Tiene la información contable más organizada en el software contable Helisa. Además, no puede acceder al aplicativo sin autorización.	Software Helisa	
	Tiene la información del centro de documentación en un sistema de información. Tiene restricciones de ingreso.	Base de datos CD	

	Mantenimiento preventivo y correctivo actualizado con roles, responsabilidades y fechas.	Buen funcimiento de los equipos.	
	Gestión de seguridad	Abarca todo el tema de seguridad de la información e informática de la entidad.	

4.8. MARCO CIENTÍFICO O TECNOLÓGICO

Para Graells (2000), las TICs son un conjunto de avances tecnológicos posibilitados por la informática, las telecomunicaciones y las tecnologías audiovisuales, todas éstas proporcionan herramientas para el tratamiento y la difusión de la información y contar con diversos canales de comunicación. El elemento más poderoso que integra las TICs es la Internet, que ha llevado a la configuración de la llamada Sociedad de la Información, el autor indica que ésta posibilita la existencia de un tercer mundo, donde se puede hacer casi todo lo que se hace en el mundo "físico", un segundo mundo sería el de la imaginación.[12]

4.8.1. Tecnología: herramienta wappalyzer

"Se trata de una extensión de código abierto gratuita para navegadores que descubre las tecnologías utilizadas en los sitios web.
Es capaz de identificar 1,222 tecnologías web en 65 categorías diferentes. Detecta patrones únicos que se encuentran en el código fuente de un sitio web, encabezados de respuesta, variables de script y varios otros métodos de forma que es capaz de saber los sistemas de administración de contenido, plataformas de comercio electrónico, marcos web, software de servidor, herramientas de análisis, etc. con los que cuenta una web."[13]

4.8.2. Tecnología CVE MITRE.

"CVE El código CVE (vulnerabilidades y amenazas comunes) es un identificador que se asigna a cada vulnerabilidad que se conoce públicamente con el fin de que pueda ser identificada de forma unívoca (The MITRE Corporation, 2011). Este código fue creado por la corporación MITRE y permite que los usuarios puedan conocer de forma objetiva las vulnerabilidades de un sistema computacional. Los identificadores CVE se presentan en el formato CVE-AÑO-NUMERO y están

[12] (LAS TIC, s.f.)
[13] (Caballero, 2019)

acompañados de una breve descripción de la vulnerabilidad o amenaza y un grupo de referencias pertinentes."[14]

4.8.3. Tecnología CVSS.

"Sistema común de puntuación de vulnerabilidades CVSS (Mell et al., 2007) es un sistema de puntuación de vulnerabilidades diseñado con el fin de proporcionar un método abierto y estandarizado para la clasificación de vulnerabilidades en tecnologías de la información. Con esto ayuda a las organizaciones a priorizar y coordinar una respuesta concertada para la mitigación de vulnerabilidades de TIC. Adicionalmente CVSS provee a profesionales en seguridad informática, ejecutivos y usuarios finales un lenguaje común para discutir la severidad de las vulnerabilidades de seguridad."[15]

4.9. MARCO LEGAL

En este capítulo se exponen las diferentes normas Institucionales.

LEY 99 DE 1993. FUNDAMENTO DE LA POLÍTICA AMBIENTAL COLOMBIANA

Por la cual se crea el Ministerio del Medio Ambiente, se reordena el Sector Público encargado de la gestión y conservación del medio ambiente y los recursos naturales renovables, se organiza el Sistema Nacional Ambiental, SINA, y se dictan otras disposiciones.

ARTÍCULO 1o. NATURALEZA Y RÉGIMEN JURÍDICO APLICABLE. En virtud de la Ley 99 de 1.993, se crea el Instituto de Investigaciones Ambientales del Pacífico "John Von Neumann", el cual se organiza como una Corporación Civil sin ánimo de lucro, de carácter público pero sometida a las reglas de derecho privado, organizada en los términos establecidos por la Ley 29 de 1990 y el Decreto 393 de 1.991, vinculada al Ministerio de Ambiente y Desarrollo Sostenible con autonomía administrativa, personería jurídica y patrimonio propio.

Al instituto se le aplicarán, en lo pertinente, la Ley 99 de 1993, el Decreto 1603 de 1994 y en especial la Ley 21 de 1991, la Ley 70 de 1993, la Ley 160 de 1994, el Decreto 2164 de 1995, el Decreto 1745 de 1995, Decreto 2370 de 2009, la ley 1286 de 2009 y demás disposiciones que le sean aplicables.

LEY ESTATUTARIA 1266 DEL 31 DE DICIEMBRE DE 2008

[14] (Franco, Perea, & Tovar, 2013)
[15] Ibid.

Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

LEY ESTATUTARIA 1581 DE 2012

Entró en vigor 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.

Como resultado de la sanción de la anunciada ley toda entidad pública o privada, cuenta con un plazo de seis meses para crear sus propias políticas internas de manejo de datos personales, establecer procedimientos adecuados para la atención de peticiones, quejas y reclamos, así como ajustar todos los procesos, contratos y autorizaciones a las disposiciones de la nueva norma.[16]

LEY 1273 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."[17]

Capitulo I. De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos

Artículo 269A: Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.[18]

Artículo 269D: Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena

---

[16] CAMELO, L. Seguridad de la Información en Colombia. Obtenido de Marco legal de Seguridad de la Información en Colombia. Colombia: 2010

[17] CONGRESO DE COLOMBIA. Ley 1273 de 2009 en COLOMBIA: de la protección de la información y de los datos, 2009. p. 2.

[18] ibíd.

de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.[19]

Artículo 269C: Interceptación de datos informáticos. "El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses."[20]

Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.[21]

5. DISEÑO METODOLÓGICO

5.1. METODOLOGÍA

La metodología por utilizar para conocer el estado actual de la seguridad de los activos de información frente a vulnerabilidades o ataques.

Se procura identificar, vulnerabilidades y amenazas, a las que se expone la información institucional a la hora de procesar, transportar, almacenar y la disposición final de la información.

Para emprender esta metodología se tiene cuenta 3 aspectos:

- Diagnóstico
- Análisis con Magerit
- Escaneo de vulnerabilidades

5.1.1. DIAGNÓSTICO.

Tiene como principio realizar una evaluación del estado de seguridad informática a todos los activos de la institución

[19] Ibíd.
[20] ibíd.
[21] ibíd.

En concordancia, se toma como referencia los controles de la norma Técnica Colombiana NTC ISO/IEC 27001:2013, diagnóstico de la seguridad de la información y el resultado de las encuestas. (ver anexo G)

Dentro de los controles están:

- **Políticas de la seguridad de la información**

Elaboración: Propia del autor.

A.5	**POLITICAS DE SEGURIDAD**	0	No existe	0%	**Objetivo:** Apoyar al área TIC en la seguridad de la información de acuerdo con los requisitos, leyes y reglamentos pertinentes.
A.5.1	**Políticas de seguridad de la información**	0	No existe	0%	
A.5.1.1	Documento de política de seguridad de la información	0	No existe	0%	**Control:** Se deben establecer políticas para la seguridad de la información, aprobada por el coordinador del área TIC, planeación y dirección del instituto de Investigaciones Ambientales del Pacifico para luego ser publicada y comunicada Con todos los usuarios de la misma.
A.5.1.2	Revisión de las políticas	0	No existe	0%	**Control:** Las políticas para seguridad de la información se deben presentar para una previa revisión donde participen las áreas de planeación, TIC y dirección, con sus cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas

Se evidencia que es un proceso inexistente, dentro de las recomendaciones o control se deben establecer políticas de seguridad de la información para proteger referente principal de la entidad con definición de roles y responsabilidades.

- **Aspectos organizativos de la seguridad de la información.**

Elaboración: propia del autor

A.6	**ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD DE LA INFORMACIÒN**	1	Etapa inicial	10%	**Objetivo:** Organizar todo lo que respecta a la seguridad de la información desde el área TIC y socializarlo con la alta gerencia y demás dependencias del Instituto de Investigaciones Ambientales del Pacifico.
A.6.1	**Organización Interna**	1	Etapa inicial		
A.6.1.1	Compromiso de la alta dirección con la seguridad de la información.	1	Etapa inicial	10%	Desde la alta dirección se debe dar más importancia al proyecto de la seguridad de la información.
A.6.1.2	Coordinación de la seguridad de la información.	1	Etapa inicial	10%	
A.6.1.3	Asignación de roles	0	No existe	0%	
A.6.1.4	Acuerdos de confidencialidad.	0	No existe	0%	
A.6.1.5	Contacto con las autoridades	0	No existe	0%	
A.6.1.6	Revisión independiente de la seguridad de la información.	0	No existe	0%	

En organización interna de la entidad se encuentra en una la etapa inicial, lo que demuestra el interés y compromiso por la alta dirección en la implementación de la seguridad de la información, aunque tiene aspectos que no han sido definidos como la asignación de roles, contactos con autoridades que puedan ayudar a detectar alguna vulnerabilidad y hacer su respectivo procedimiento legal.

- **Gestión de activos**

Elaboración: propia del autor.

A.7	**GESTION DE ACTIVOS**	0.3	No existe	0%	**Objetivo:** Identificar los activos de información institucionales. **Control:** identificar los activos de información, los activos tecnológicos y elaborar el inventario de acuerdo a la guía y matriz de Inventario y clasificación de los activos de información realizada por el área TIC (ver guía y matriz en anexo C Y D)
A.7.1	**Responsabilidad de activos**	0	No existe	0%	**Control:** Cada activo debe tener su responsable o doliente capaz de responder ante el área TIC.
A.7.1.1	Inventario de activos	0	No existe	0%	**Control:** identificar los activos de información, los activos tecnológicos y elaborar el inventario de acuerdo a la guía y matriz de Inventario y clasificación de los activos de información realizada por el área TIC (ver guía y matriz en anexo C Y D)
A.7.1.2	Propiedad de los activos	0	No existe	0%	
A.7.2	**Clasificación de la información**	0.5	No existe	10%	**Objetivo:** Asegurar que la información se le dé el trato de seguridad adecuado. **Control:** La información se debe clasificar de acuerdo con la confidencialidad, disponibilidad integridad y criticidad.
A.7.2.1	Directrices de clasificación.		No existe	0%	

Es preocupante que la entidad no tenga definido la gestión de activos, donde se evidencie el inventario de activos, propietario y la clasificación de la información.

Lo que puede ocurrir es perdida de información o modificación de información sin control alguno.

- **Seguridad ligada a los recursos humanos**

Elaboración: Propia del autor

A.8	**SEGURIDAD A LOS RECURSOS HUMANOS**	1.7	Etapa Inicial	10%	
A.8.1	**Antes del empleo**	2.0	Etapa media	50%	
A.8.1.1	Funciones y responsabilidades	3	Definido	90%	
A.8.1.2	Investigación de Antecedentes	0	No Existe	0%	
A.8.1.3	Términos y condiciones de contratación	3	Definido	90%	
A.8.2	**Durante el empleo**	2.0	Etapa Media	50%	
A.8.2.1	Responsabilidades de la dirección	3	Definido	90%	
A.8.2.2	Capacitación en seguridad de la información.	0	No existe	0%	
A.8.2.3	Proceso disciplinario	3	Definido	90%	
A.8.3	**Cese de empleo**	1.0	Etapa Inicial	10%	
A.8.3.1	Responsabilidad de cese o cambio de empleo	0	No existe	0%	
A.8.3.2	Devolución de activos	1	Etapa inicial	10%	
A.8.3.3	Retirada de los derechos de acceso	2	Etapa media	50%	

La seguridad da lo recursos humanos esta en su etapa inicial, lo que se puede evidenciar, que han venido trabajando en todo el proceso de la contratación y seguridad de la información de los empleados.

- **Seguridad Física y del entorno**

Elaboración: Propia del autor

A.9	**SEGURIDAD FISICA Y DEL ENTORNO**	1.2	Etapa Inicial	10%	
A.9.1	**Áreas seguras**	1.0	Etapa inicial	10%	
A.9.1.1	Controles de entrada	0	No existe	0%	
A.9.1.2	Seguridad de Oficinas	1	Etapa inicial	10%	
A.9.1.3	Protección contra las amenazas externas y de origen ambiental	0	No existe	0%	No existe ninguna protección contra amenazas de origen ambiental
A.9.1.4	Trabajo en áreas seguras	1	Etapa inicial	10%	
A.9.2	**Seguridad de los Equipos de tecnología**	1.3	Etapa inicial	10%	
A.9.2.1	Seguridad del cableado	2	Etapa media	50%	
A.9.2.2	Seguridad de los equipos fuera de las instalaciones	0	No existe	0%	
A.9.2.3	Reutilización o retirada de los equipos	2	Etapa media	50%	

En este control se logra evidenciar que, aunque este en etapa inicial deberán de trabajarle más en la seguridad de los equipos como los servidores que están desprotegido en caso de emergencia climática, el cableado para evitar accidentes, y los equipos que salen de las instalaciones para un control y cuidados de estos.

- **Gestión de comunicaciones y operaciones**

Elaboración: Propia del autor.

A.10	**GESTION DE COMUNICACIONES Y OPERACIONES**	1.0	Etapa inicial	10%	
A.10.1	**Protección contra códigos Maliciosos.**	0	No existe	0%	**Control:** Certificar que la información este protegida contra códigos maliciosos. **Control:** Implementar controles de seguridad dirigidos por el área TIC en contra de códigos maliciosos.
A.10.1.1	Controles contra códigos maliciosos	0	No tiene	0%	
A.10.2	**Copias de Seguridad**	1	Etapa Inicial	10%	**Objetivo:** Proteger la información de pérdidas. **Control:** Realizar copias de seguridad a los activos de información según lo estipulado en el plan de respaldo de información.
A.10.2.1	Copias de seguridad de la información.	1	Etapa inicial	**10%**	Se realizan copias de seguridad cuando el usuario lo solicite, no hay un cronograma definido para las copias de seguridad.

En este control se evidencia que aunque tenga una etapa inicial de las copias de seguridad de la información, no tiene una seguridad contra códigos maliciosos ni políticas que determinen que hacer en caso de ataques cibernéticos.

- **Control de acceso**

Elaboración: Propia del autor.

A.11	**CONTROL DE ACCESO**	0,3	No existe	0%	
A.11.1	**Requisitos de negocio para el control de acceso**	0,0	No existe	0%	
A.11.1.1	Política de control de acceso	0	No existe	0%	
A.11.2	**Gestión de acceso de usuarios**	**1,0**	**Etapa inicial**	**10%**	
A.11.2.1	Registro de usuarios	1	Etapa inicial	10%	
A.11.2.2	Gestión de privilegios	0	No existe	0%	
A.11.2.3	Gestión de contraseñas de usuarios	1	Etapa inicial	10%	

A.11.3	**Responsabilidades de usuarios**	**0,5**	**No existe**	**0%**	
A.11.3.1	Uso de contraseñas	1	Etapa inicial	10%	
A.11.3.2	Política de puesto de trabajo despejado y pantalla limpia	0	No existe	0%	
A.11.4	**Control de acceso a la red**	**0,0**	**No existe**	**0%**	
A.11.4.1	Política de uso de los servicios de red	0	No existe	0%	
A.11.4.2	Control de conexión a la red	0	No existe	0%	
A.11.5	**Control de acceso al sistema operativo**	**0,0**	**No existe**	**0%**	
A.11.5.1	Procedimiento seguro de inicio de sección	0	No existe	0%	
A.11.5.2	Identificación y autenticación de usuarios	0	No existe	0%	

La entidad no tiene definido la seguridad de control de acceso a sistemas operativos, sistemas de información, ni a la red institucional lo que deje en evidencia que cualquier persona puede ingresar, realizar cambios de contraseñas en los equipos, ingresar a la red conectarse y bloquear cuentas y demás. El control da como resultado no existente.

- **Adquisición, desarrollo y mantenimiento de los sistemas**

Elaboración: Propia del autor.

A.12	**ADQUISICIÒN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÒN.**	0	No existe		
A.12.1	**Controles Criptográficos.**	0%	No existe	0%	
A.12.1.1	Política del uso de los controles criptográficos.	0	No existe	0%	
A.12.1.2	Gestión clave	0	No existe	0%	

El control de adquisicion, desarrollo y mantenimiento de sistemas de informacion es inexistente, es decir, no se tiene control criptograficos ni gestion de claves. Para recomendación a la entidad se debe trabajar en este control para que la gestiòn de las claves sea eficiente.

- **Gestión de incidentes en la seguridad de la información**

Elaboración: Propia del autor

A.13	**GESTION DE INCIDENTES EN LA SEGURIDA DE LA INFORMACIÓN.**	0%	No existe	0%	
A.13.1	**Notificación de eventos**	0%	No existe	0%	
A.13.1.1	Notificación de eventos de seguridad de la información	0	No existe	0%	
A.13.1.2	notificación de puntos débiles	0	No existe	0%	
A.13.2	**Gestión de incidentes**	0%	No existe	0%	
A.13.2.1	Responsabilidades y procedimientos	0	No existe	0%	
A.13.2.2	Aprendizaje de los incidentes de seguridad.	0	No existe	0%	
A.13.2.3	Recopilación de evidencias.	0	No existe	0%	

De acuerdo con los resultados este control es inexistente, no existe un documento o políticas sobre la gestión de incidentes. En caso de ocurrir un ataque no tiene planteado como responder ante estos casos. Eso deja evidencia que falta mas compromiso y desarrollo en todo el tema de seguridad de la información.

- **Gestión de la continuidad del negocio.**

Elaboración: Propia del autor.

A.14	**GESTION DE LA CONTINUIDAD DEL NEGOCIO.**	0,5%	No tiene	0%	
A.14.1	**Aspecto de la seguridad de la información**	0	No tiene	0%	
A.14.1.1	Continuidad del negocio y evaluación de riesgos.	1	Etapa inicial	10%	

No hay seguridad en la continuidad del negocio, es decir en evaluar los riesgos, en mantener la seguridad de la información. Lo que impide seguir con el planteamiento de resguardar toda la información como activo mayor de la entidad.

- **Cumplimiento**

Elaboración: Propia del Autor.

A.15	**CUMPLIMIENTO**	1%	Etapa inicial	10%	
A.15.1	**Cumplimiento de las políticas**	0%	No existe	0%	
A.15.1.1	Cumplimiento de las políticas de seguridad	0	No existe	0%	
A.15.1.2	comprobación de cumplimiento técnico	0	No existe	0%	
A.15.2	**Auditorias de los sistemas de información**	3,0	Definido	90%	
A.15.2.1	Controles de auditoría de los sistemas de información	3	Definido	90%	

Del control de cumplimiento solo se tiene en etapa inicial las auditorias a los sistemas de información realizado por el personal de control interno de la entidad, pero es ineficiente el cumplimiento de las pocas políticas establecidas en cuanto a la seguridad.

- **Relación con los proveedores.**

Elaboración: Propia del autor.

A.16	**RELACION CON LOS PROVEEDORES**	0%	No existe	0%	
A.16.1	Seguridad con los proveedores	0%	No existe	0%	
A.16.2	Gestión de servicios externos.	0%	No existe	0%	

En relación con los proveedores no existe gestión de servicios externo y tampoco se tiene establecido seguridad con los proveedores de los equipos tecnológicos.

En conclusión, y de acuerdo con la referencia de los controles de la Norma Técnica Colombiana NTC ISO/IEC 27001:2013 listadas anteriormente.

El Instituto de Investigaciones Ambientales del pacifico en el ámbito de seguridad, no cuenta con políticas que respalden la seguridad de la información como activo más importante de la misma.

Los equipos de cómputo no cuentan con seguridad lógica es decir cualquier usuario puede ingresar y manipular la información.

No cumple con la definición de roles y responsabilidad para atender casos de incidencias en cuanto a la seguridad.

Se propone realizar cada una de las actividades para asegurar los activos y tener un plan de seguridad informática como lo exige el Ministerio de las TIC a nivel nacional lo que contribuye a la seguridad digital.

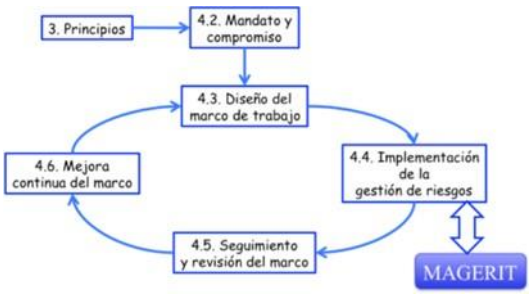
5.1.2. ANÁLISIS – MAGERIT.

Existen 4 pasos para el análisis de riesgos

1. Identificar los riesgos
2. Determinar al nivel de criticidad de cada riesgo
3. Clasificar los riesgos, donde se toma como referencia el proceso Magerit
4. Determinar las acciones necesarias.

Proceso Magerit.

Figura 3. Proceso Magerit



5.1.3. ESCANEO DE VULNERABILIDADES.

Se utilizan las herramientas wappalyzer y OWASP ZAP versión 2.11 para identificar las posibles vulnerabilidades que afectan a los activos de información y definir controles de acuerdo a la ISO 27001.

Resultados:

Se realizo una prueba de escaneo de seguridad al sitio web del Instituto de Investigaciones Ambientales del Pacifico con las siguientes herramientas:

- Con la herramienta wappalyzer instalada en el explorar de Google Chrome. “Wappalyzer es una extensión del navegador que descubre las tecnologías utilizadas en los sitios web. Detecta sistemas de administración de contenido, tiendas web, servidores web, marcos de JavaScript, herramientas de análisis y muchos más.”

En resumen, el sitio web tiene apache 2.4.29, sistema operativo Ubuntu con una tipografía de Google Font API que admite archivos de código abierto para su diseño.

por consiguiente y analizar más de fondo las vulnerabilidades del servidor utilizado por la página web del IIAP apache 2.4.29 se encontraron 4 vulnerabilidades con el análisis de CVI METRI con los siguientes resultados:
Gravedad de vulnerabilidad alta con 8.1 lo que indica que está en riesgo la página Co unas métricas de impacto en Confidencialidad, integridad y disponibilidad altos.

También, se realizó un análisis de vulnerabilidades con la herramienta OWASP ZAP versión 2.11 la herramienta owasp zap es un escáner de seguridad con la intención de realizar pruebas de penetración para comprobar si existen vulnerabilidades.
Efectivamente el resultado fueron 10 alertas encontradas en el sitio web del IIAP dos con riesgo alto, dos riesgos medios y el demás riesgo bajo. Lo que indica que si hay riesgo de información en el sitio web y de autenticación.

El Instituto de Investigaciones Ambientales del Pacifico cuenta con un entorno físico de 2 plantas, cuanta con 1 servidor donde se almacena información solamente institucional, una UPC para regular la energía eléctrica y con 30 equipos de cómputo.

6. DETERMINAR LOS ACTIVOS DE INFORMACIÓN, LOS RIESGOS Y LAS FALLAS DE SEGURIDAD PRESENTES EN LA INFRAESTRUCTURA TECNOLÓGICA Y DE COMUNICACIONES DE LA EMPRESA.

A través del inventario de activos de información se identifican cuáles son los activos más importantes para el Instituto de Investigaciones Ambientales del Pacifico para implementar la protección adecuada, para el cumplimiento de la misión y los objetivos institucionales. El inventario permite equiparar los activos de información a los que se les brinda mayor protección y que se pueden requerir para actividades propias de la Institución.

Instituto de Investigaciones Ambientales del Pacifico, se han presentado casos de incidentes de seguridad.

Casos de Incidentes de seguridad:

- **Abuso de privilegios de acceso.** El mal manejo de las credenciales para ingresar a la base de datos provoco el desvió de información financiera.

- **Auto relleno de inicio de sesión.** El relleno automático de las credenciales al ingresar al sistema provoco un bloqueo del sistema de información integrado Helisa y no se reportó información financiera dos días

- **Falta de contraseña al inicio.** Al no tener seguridad de contraseña al iniciar sección se vio afectada la información de eliminación de algunos datos financieros por alguien que ya no hacia parte de la institución.

- **Correos electrónicos con link de dudosa procedencia.** Al no tener cortafuego ni analizador de link, al ingresar los datos, toda esa información quedo almacenada en base de datos de ciberdelincuentes.

- **Hurto de equipos tecnológicos.** No tiene control de acceso al edificio lo que permite que cualquier usuario se lleve un bien tecnológico.

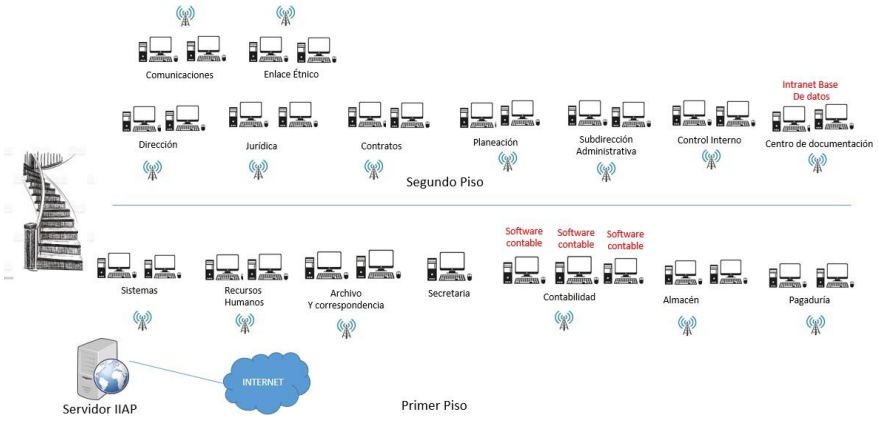
- **Perdida de información.** Las copias de seguridad las realizan cuando el usuario hace el requerimiento.

Seguido, el Instituto de Investigaciones Ambientales del Pacifico cuenta con dos sistema de información donde se almacena toda la información de los proyectos que realiza la misma, se llama centro de documentación y la información contable con el software Helisa. De acuerdo a la encuesta y análisis de seguridad realizado a todos los empleados, los resultados arrojados dieron un alto riesgo de pérdida de información y ataques de vulnerabilidades, esto se debe a que los equipos no cuentan con ningún proceso de seguridad, No tiene antivirus, los usuarios no han recibido capacitaciones sobre seguridad de la información, el acceso a la base de datos es desde la página web que también presenta vulnerabilidades e impacto de nivel Crítico en confidencialidad, integridad y disponibilidad. la información está expuesta al público lo que también coloca en riesgo todos los proyectos de investigación.

Los usuarios tienen la clave de fácil acceso para terceros lo que implica un abuso de privilegio de acceso y pueden ocurrir vulnerabilidades y es un activo de mayor grado debido al contenido. Para poder obtener información de investigación se debe solicitar al personal encargado, pero teniendo los equipos sin seguridad de inicio cualquier usuario puede acceder a la información sin realizar una solicitud.

Se necesita más refuerzo en la seguridad de los equipos no solamente en los que contiene el software contable Helisa sino en todos para brindar una mayor seguridad a los activos tecnológicos y de información.

Infraestructura tecnológica

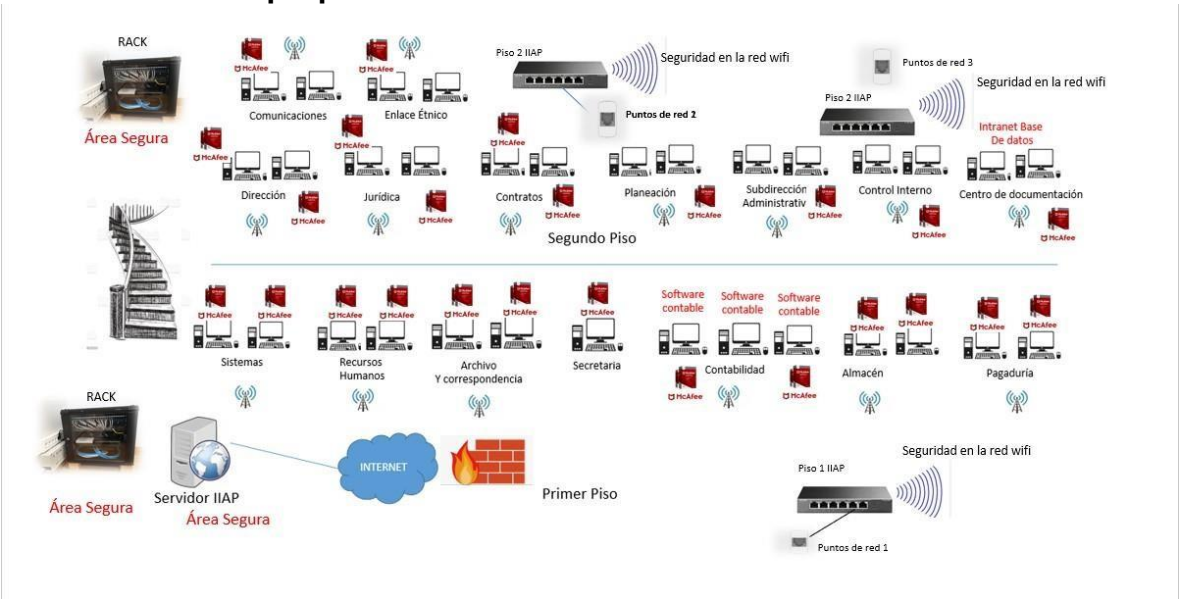


propia del autor.

De los riesgos a nivel de infraestructura están los servidores que se encuentran ubicados en el primero piso del edificio expuestos a inundaciones. El Rack donde están las conexiones de internet esta debajo de un aire acondicionado expuesto a humedad lo que pone en riesgo la conexión. Además, no tiene señalización de salida de emergencia y extintores en caso de incendios.

Para lo expuesto anteriormente y mejorar la infraestructura tecnológica del Instituto de Investigaciones Ambientales del Pacifico se propone la siguiente de acuerdo con los resultados de las encuesta y análisis de seguridad.

Topología propuesta para el Instituto de Investigaciones Ambientales del Pacifico. Fuente: propia del autor.



7. EVALUAR LOS RIESGOS DE ACUERDO CON LA PROBABILIDAD DE OCURRENCIA Y AL IMPACTO CONSIDERANDO LAS AMENAZAS Y VULNERABILIDADES.

7.1. METODOLOGÍA PARA EL RIESGO.

En la siguiente figura se visiona el proceso general del análisis de riesgos junto con el proceso de seguridad de la información que consta de 4 componentes:

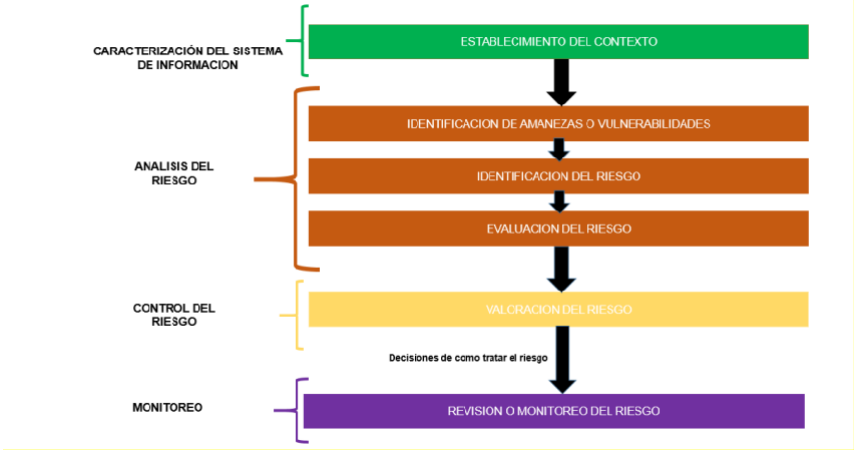
- **Caracterización.** Conocimiento de todas las actividades, es decir el contexto de la situación para luego seguir con el análisis del riesgo.

- **Análisis del riesgo.** como su nombre lo indica es el análisis de los riesgos y sus posibles consecuencias; con el objetivo de instaurar medidas de prevención y protección de los activos. En este proceso se identifican las amenazas o vulnerabilidades, identificación del riesgo y evaluación del riesgo.

- **Control del riesgo.** Es la valoración del riesgo donde se instauran medidas de seguridad obtenidas de la evaluación o análisis del riesgo donde se aplican factores ergonómicos, psicosociales y riesgos del entorno.

- **Monitoreo.** Es la actividad continua que permite la administración para identificar riesgos críticos de manera apropia, oportuna y eficiente.

Figura 4. Proceso de Análisis de Riesgo



Propia del Autor

Un análisis cuantitativo o cualitativo se le define como análisis de riesgo dando como resultado la evaluación del riesgo. Al ocurrir riesgo se estaría comprometiendo la Confidencialidad, integridad y disponibilidad de la información.

7.1.1. Análisis del Riesgo.

En esta fase se deben evaluar los riesgos identificados, con el objetivo de establecer la probabilidad y el impacto de los mismos.
También, el responsable o custodio de la información debe identificar las amenazas, vulnerabilidades y riesgo a los que se expone la misma. Para garantizar la disponibilidad, confidencialidad e integridad.

Se debe tener en cuenta:

- Identificar cuáles son los riesgos que pueden afectar la misión y visión institucional.
- Amenazas y vulnerabilidades.
- El impacto que se generaría al confirmarse una o más amenazas Identificadas
- La probabilidad de que dicho riesgo se realice.

En continuidad, se visiona la tabla de riesgos, en el cual se deben ubicar los riesgos identificados y su nivel de probabilidad e impacto.

Tabla 1. Tabla de riesgos

PROBABILIDAD	IMPACTO				
	Insignificante	Menor	Medio	Mayor	Catastrófico
Raro	B	B	B	M	M
Improbable	B	M	M	A	A
Moderado	B	M	A	A	E
Probable	M	A	A	E	E
Casi certeza	M	A	E	E	E

Fuente: propia del autor.

Color	Zona de riesgo

B	Zona de riesgo baja
M	Zona de riesgo medio
A	Zona de riesgo alta
E	Zona de riesgo extrema

Fuente: propia del autor.

7.1.1.1. Identificación de Amenazas.

Las amenazas pueden ocasionar daños a los activos identificados y afectar de una u otra manera los objetivos, misión y actividades de la institución.

Las amenazas pueden ser:

Ataques
Errores humanos
De origen industrial
De origen natural

7.1.1.2. Identificación de los activos.

Se rige bajo la norma ISO 27000:2013Los activos de información son la parte fundamental de una empresa u organización en este caso de la institución. Por ende, se deben identificar cada uno de los activos que representen una actividad esencial en el instituto. Se realiza mediante una matriz de identificación y clasificación de activos de información.

7.1.1.3. Identificación de amenaza.

Una amenaza tiene el peso de causar daños informáticos, daños en activos de la información y en proceso.

Estas amenazas pueden ser de origen natural o humano. Por eso es importante identificar todos los orígenes de estas.

Algunas amenazas más comunes:

Tabla 2. Tabla de amenazas más comunes

TIPO	AMENAZA
Daño físico	Fuego Agua Contaminación Accidente importante Destrucción de equipos

Eventos naturales	Fenómenos climáticos Fenómenos sísmicos Inundación
De la información	Hurto de medios o documentos Hurto de equipo Datos provenientes de fuentes no Confiables Manipulación con hardware Manipulación con software
Fallas Técnicas	Fallas del equipo Mal funcionamiento del equipo Mal funcionamiento del software Incumplimiento en el mantenimiento del sistema de información.
Actividades no deseadas	Uso no autorizado del equipo Copia fraudulenta del software Uso de software falso o copiado Procesamiento ilegal de datos

7.1.1.4. Identificación de Vulnerabilidades.

Las vulnerabilidades causan daño al activo a menos que haya una amenaza presente.

7.1.1.5. Identificación del Riesgo.

De acuerdo con las amenazas y vulnerabilidades que se identifican se puede determinar el riesgo de los activos de información. Dichas fallas se pueden ver afectadas por el incumplimiento de los objetivos si en un caso dado se materializan las amenazas.

7.1.1.6. Estimación del Riesgo.

Para una estimación del riesgo se debe calificar la probabilidad de 1 a 5 con la que se puede materializar la amenaza. También, se debe calificar el impacto en una escala de 1 a 5 de acuerdo con la amenaza. Dando así un nivel del riesgo para luego actuar bajo los controles de seguridad.

7.1.1.7. Evaluación del Riesgo.

Una vez se identifique el riesgo se debe evaluar el mismo para saber cómo atacar o minimizar

7.1.1.8. Tratamiento del Riesgo.

En esta fase se debe tomar decisiones sobre cómo será el tratamiento del riesgo o amenaza.

7.1.1.9. Identificación de las consecuencias

Se debe tener en cuenta para la identificación de las consecuencias lo siguiente:

- Activos de información, procesos, responsables, custodios y almacenamiento de la información.
- Amenazas y vulnerabilidades en cuanto a los activos

7.1.1.10. Enfoque de mitigación.

En este último paso, se determina las alternativas de riesgo de acuerdo a los resultados del análisis utilizando valores del impacto y probabilidad.

7.1.1.11. Nivel de Criticidad de cada riesgo.

Se prioriza los riesgos a tratar teniendo en cuenta los problemas de seguridad de la entidad, por lo que se puede utilizar los registros de incidentes.

A una probabilidad de ocurrencia alta se le asigna un valor de 3, si es media un valor de 2 y si es 1 para una probabilidad baja.

En este paso se mide de forma cualitativa el grado de afectación de la entidad por una amenaza y se conjetura una puntuación para cada riesgo de cada activo de información.

CUADRO 3. De acuerdo con la integridad

INTEGRIDAD		
VALOR	**NIVEL**	**DESCRIPCION**
3	**ALTA**	La información se debe resguardar de toda perdida de exactitud para no tener un impacto negativo, ni retrasar las funciones o procesos de la entidad.
2	**MEDIA**	La información se debe resguardar de toda perdida de exactitud para no tener un impacto negativo, ni retrasar las actividades de la entidad.
1	**BAJA**	En este punto, la perdida exactitud de la información no conlleva a un impacto tan alto como los niveles anteriores.

Propia del autor

CUADRO 4. De acuerdo con la confidencialidad

CONFIDENCIALIDAD			
PUBLICA RESERVADA.	**PUBLICA CLASIFICADA**	PUBLICA	NO CLASIFICADA
NIVEL 3 ALTA	**NIVEL MEDIO 2**	NIVEL BAJO 1	
Información solo para asuntos de la entidad. Al ser evaluada por terceros sin autorización conlleva a un proceso legal por parte de la entidad. ley 1712 de 2014 en el artículo 19	Información propia de la entidad, puede ser compartida por los empleados de la misma y a terceros, pero con autorización del propietario. ley 1712 de 2014 en el artículo 18	Información que es presentada al público sin restricción alguna. ley 1712 de 2014 del artículo 24	Información que se debe tener en cuenta en los activos de información, aunque no haya sigo clasificada.

propia del autor

CUADRO 5. De acuerdo con la disponibilidad

DISPONIBILIDAD		
VALOR	**NIVEL**	**DESCRIPCION**
3	ALTA	La falta o no disponibilidad del activo de información impacta negativamente la prestación del servicio y a la entidad. Ley 1581 de 2012
2	MEDIA	La falta o no disponibilidad del activo impacta negativamente los procesos o actividades de

		la entidad. Ley 1581 de 2012
1	BAJA	La falta o no disponibilidad del activo el impacto es mínimo. Ley 1581 de 2012

Propia del autor.

CUADRO 6. De acuerdo con la Criticidad

CRITCIDAD				
M	M	A	A	A
M	M	A	A	A
B	M	M	A	A
B	B	M	M	A

propia del autor

CLASIFICACIÓN DEL RIESGO

Tabla 3. Clasificación del riesgo

RIESGO	EJEMPLO
Físico	Ruido, iluminación, temperaturas, radiación, humedad.
Biológico	Virus, hongos, bacteria
Químico	Gases, vapores, polvo, líquidos
De seguridad	Mecánicos, eléctricos
Lógicos	Códigos maliciosos, spam, intrusos informáticos, Ingeniería social, fuga de información.

Tipos de riesgo:

Riesgo Alto. Cuando la amenaza representa un impacto de gran importancia sobre los activos de información.

Riesgo Medio. La amenaza es parcial para los activos de información

Riesgo bajo. La amenaza no representa ningún peligro

Para la evaluación de los riesgos de acuerdo con probabilidad de ocurrencia y al impacto considerando las amenazas y vulnerabilidades se tiene en cuanta el resultado de las encuestas y el análisis de vulnerabilidades a la que se enfrentan el IIAP en los equipos de cómputos, base de datos del centro de documentación donde reposan los archivos de proyectos realizados por la entidad y la página web.

En la cuesta consta de 14 preguntas:

1. ¿Existe un área o encargado de la seguridad informática?
2. ¿Han tenido problemas de seguridad donde se haya visto comprometida la información o proyectos de la entidad?
3. Si tu respuesta anterior fue SI, explica cuáles han sido los problemas de seguridad.
4. ¿Cuál de estos navegadores utilizas más?
5. ¿Tu computadora tiene software antivirus instalado?
6. ¿Cuál de este software antivirus utilizas o conoces?
7. ¿Conoces algún Cronograma de mantenimiento en la entidad?
8. ¿Realizan manteamiento preventivo y/o correctivo a las computadoras?
9. ¿Cada cuando realizan el mantenimiento a los equipos de cómputos?
10. ¿Realizan copias de seguridad?
11. ¿Cada cuanto realizan copias de seguridad a la información?
12. ¿Qué método de seguridad utilizan para los equipos de cómputos de la entidad?
13. ¿Tienes seguridad para protección de tus activos de información?
14. ¿Han compartido documentos o charlas sobre seguridad informática?

Como resultado, el Instituto de Investigaciones Ambientales del Pacifico

- No tiene definido el paso a paso para realizar copias de seguridad lo que lleva a un impacto negativo en perdida de información por daño de disco duro sin respaldo

- No se ejecuta correctamente el cronograma de mantenimiento preventivo/correctivo

- Los empleados no tienen conocimiento sobre seguridad de la información por falta de capacitaciones o charlas.

- Algunos equipos de cómputos no tienen antivirus instalado.

- No tiene seguridad de contraseñas o reconocimiento facial.

- La entidad no tiene definido roles ni responsabilidades de la seguridad informática y las respuestas a incidentes.

- No tiene Definido las acciones a implementar a nivel de seguridad y privacidad, así como acciones de mitigación del riesgo.

- entidad no implementa el plan de seguridad y privacidad de la información, clasifica y gestiona controles

- La entidad no cuenta con actividades para el seguimiento, medición, análisis y evaluación del desempeño de la seguridad y privacidad a efecto de generar los ajustes o cambios pertinentes y oportunos

- No implementan un plan de mejoras continuas.

- La entidad no cuenta con políticas definidas sobre seguridad informática.

Acto seguido, Los equipos de cómputo, en especial donde reposa información institucional de gran importancia no cuentan con seguridad lógica, es decir, cualquier usuario puede ingresar y manipular la información, no tienen contraseña, ni restricción al descargar y ejecutar programas.

Se realizo una prueba de escaneo de seguridad al sitio web del Instituto de Investigaciones Ambientales del Pacifico con las siguientes herramientas:

- Con la herramienta wappalyzer instalada en el explorar de Google Chrome. "Wappalyzer es una extensión del navegador que descubre las tecnologías utilizadas en los sitios web. Detecta sistemas de administración de contenido, tiendas web, servidores web, marcos de JavaScript, herramientas de análisis y muchos más." [22]

En resumen, el sitio web tiene apache 2.4.29, sistema operativo Ubuntu con una tipografía de Google Font API que admite archivos de código abierto para su diseño.

[22] (Wappalyzer - Technology profiler, 2022)

Tabla 4. Diagnóstico de seguridad de la información estado del arte. Elaboración propia del autor.

PREGUNTAS DE SEGURIDAD	SI	NO	OBSERVACIONES
¿Cuenta con políticas de seguridad informática?		x	La entidad no cuenta con políticas de seguridad informática. Se plantea proponer las políticas, entregarlas a la alta gerencia para ser aprobadas.
¿tiene bitácora de copias de seguridad)	x		La entidad tiene bitácora de copias de seguridad. Se propone actualizar la bitácora basa en políticas o plan
¿Realizan copias de seguridad?	x		Cuando el empleado lo solicite. La entidad no cuenta con un plan de copias de seguridad, no tiene definido un cronograma donde se establezcan fechas y actividades de cómo se realizan las copias de seguridad. Se plantea realizar un cronograma, plan o políticas para realizar las copias de seguridad donde se explique el proceso.
¿Tienen definido como realizan las copias de seguridad?		x	No tiene definido el proceso de cómo realizar las copias de seguridad. Se propone realizar un cronograma con la definición del proceso.
¿Tienen definido los roles y responsables de la seguridad informática en la entidad?		x	La entidad no tiene definido desde que área y los responsables de la seguridad informática y las respuestas a incidentes. Se propone realizar un consejo en el área de las TIC para definir roles y responsabilidades ante cualquier dificultad o vulnerabilidad.
¿Cuenta con señalización de salida de emergencia, ni extintores en caso de incendios?		x	La entidad no tiene señalización de evacuación en temas de emergencia o desastres naturales. Se propone colocar señales de evacuación de emergencia y mas en el piso

			donde se encuentra los servidores, la UPS y demás equipos.
¿Tienen inventariado la información?		x	La entidad no tiene un inventario de activos de información. Se plantea realizar un inventario de la información basado en la norma ISO 27001
¿Tienen plan de capacitación?		x	La entidad no cuenta con plan de capacitación en las TIC. Se plantea implementar un plan de capacitación en herramientas TIC
¿Han realizado capacitaciones o charlas sobre seguridad informática?		x	El área TIC no han realizado charlas ni capacitaciones sobre seguridad informática. Se requiere realizar charlas o capacitaciones sobre seguridad informática donde se les de a conocer que hacer en caso de una vulnerabilidad o ataque cibernético.
¿Cuentan con políticas de seguridad?		x	La entidad no cuenta con políticas definidas sobre seguridad informática. Se proponen establecer políticas y socializarlas con la alta gerencia para su cumplimiento.
¿Tienen directorio activo?		x	La entidad no tiene directorio activo.
¿Tiene algún documento que defina como abordar los incidentes de seguridad informática?		x	La entidad no tiene documentos donde se defina como abordar casos de incidencias. Se propone realizar un documento con el paso a paso de cómo abordar incidencias de seguridad.
¿Realizan mantenimiento preventivo y correctivo a los equipos de cómputo?	x		La entidad realiza mantenimiento preventivo y correctivo a los equipos cuando el usuario lo necesita o haga el requerimiento.
¿La entidad cuenta con un diagnóstico de seguridad y privacidad e identifica y analiza los riesgos existentes?		x	No cuenta con un diagnóstico de seguridad. Se propone realizar un diagnóstico con encuestas, análisis de brecha.

¿La entidad define las acciones a implementar a nivel de seguridad y privacidad, así como acciones de mitigación del riesgo?		x	No define ningunas acciones de seguridad ni para mitigar el riesgo. Se plantea realizar un documento donde se definen acciones ante vulnerabilidades.
¿La entidad implementa el plan de seguridad y privacidad de la información, clasifica y gestiona controles?		x	No implementa plan de seguridad ni gestión de controles ISO 27001. Es necesario que se implemente un plan de seguridad y privacidad de la información.
¿La entidad cuenta con actividades para el seguimiento, medición, análisis y evaluación del desempeño de la seguridad y privacidad a efecto de generar los ajustes o cambios pertinentes y oportunos?		x	No cuenta con actividades de seguimiento ni desempeño de la seguridad.
¿La entidad revisa e implementa acciones de mejora continua que garanticen el cumplimiento del plan de seguridad y privacidad de la Información?		x	No implementan un plan de mejoras continuas.

8. DEFINIR LOS CONTROLES, PROCEDIMIENTOS Y ESTADO ACTUAL DE LA ENTIDAD PARA EL TRATAMIENTO EFECTIVO DE LOS RIESGOS Y VULNERABILIDADES DE ACUERDO CON LA ISO 27001.

La siguiente tabla detalla los controles, los dominios definidos en el componente de Planificación. Tomando en cuenta el Anexo A de la norma NTC: ISO/IEC 27001.

Modelo de tabla tomada de la guía Controles de Seguridad y Privacidad de la Información realizada por Ministerio de las TIC basada en el anexo A de la ISO 27001.

TABLA 5. Niveles de madurez para el análisis brecha o GAP. Fuente: propia del autor

Porcentaje nivel de cumplimiento	Niveles	Descripción
0%	0	No existe.
10%	1	Etapa inicial
50%	2	Etapa media
90%	3	Definido
95%	4	Medible y manipulable
100%	5	Optimizado

Núm.	Nombre	Nivel	estado	Cumplimiento	Descripción / Justificación
	Objeto y campo de aplicación				Seleccionar los controles para el tratamiento efectivo de los riesgos y vulnerabilidades.
	Referencia normativa				ISO 27001
A.5	**POLITICAS DE SEGURIDAD**	0	No existe	0%	**Objetivo:** Apoyar al área TIC en la seguridad de la información de acuerdo con los requisitos, leyes y reglamentos pertinentes.
A.5.1	**Políticas de seguridad de la información**	0	No existe	0%	
A.5.1.1	Documento de política de seguridad de la información	0	No existe	0%	**Control:** Se deben establecer políticas para la seguridad de la información, aprobada por el coordinador del área TIC, planeación y dirección del instituto de Investigaciones Ambientales del Pacifico para luego ser publicada y comunicada Con todos los usuarios de la misma.
A.5.1.2	Revisión de las políticas	0	No existe	0%	**Control:** Las políticas para seguridad de la información se deben presentar para una previa revisión donde participen las áreas de planeación, TIC y dirección, con sus cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.
A.6	**ASPECTOS ORGANIZATIVOS**				**Objetivo:** Organizar todo lo que respecta a la seguridad de la

	PARA LA SEGURIDAD DE LA INFORMACIÒN	1	Etapa inicial	10%	información desde el área TIC y socializarlo con la alta gerencia y demás dependencias del Instituto de Investigaciones Ambientales del Pacifico.
A.6.1	**Organización Interna**	1	Etapa inicial		
A.6.1.1	Compromiso de la alta dirección con la seguridad de la información.	1	Etapa inicial	10%	Desde la alta dirección se debe dar más importancia al proyecto de la seguridad de la información.
A.6.1.2	Coordinación de la seguridad de la información.	1	Etapa inicial	10%	
A.6.1.3	Asignación de roles	0	No existe	0%	
A.6.1.4	Acuerdos de confidencialidad.	0	No existe	0%	
A.6.1.5	Contacto con las autoridades	0	No existe	0%	
A.6.1.6	Revisión independiente de la seguridad de la información.	0	No existe	0%	
A.7	**GESTION DE ACTIVOS**	0.3	No existe	0%	**Objetivo:** Identificar los activos de información institucionales. **Control:** identificar los activos de información, los activos tecnológicos y elaborar el inventario de acuerdo a la guía y matriz de Inventario y clasificación de los activos de información realizada por el área TIC (ver guía y matriz en anexo C Y D)
A.7.1	**Responsabilidad de activos**	0	No existe	0%	**Control:** Cada activo debe tener su responsable o doliente capaz de responder ante el área TIC.
A.7.1.1	Inventario de activos	0	No existe	0%	**Control:** identificar los activos de información, los activos tecnológicos y elaborar el inventario de acuerdo a la guía y matriz de Inventario y clasificación de los activos de información realizada por el área TIC (ver guía y matriz en anexo C Y D)

A.7.1.2	Propiedad de los activos	0	No existe	0%	
A.7.2	**Clasificación de la información**	0.5	No existe	10%	**Objetivo:** Asegurar que la información se le dé el trato de seguridad adecuado. **Control:** La información se debe clasificar de acuerdo con la confidencialidad, disponibilidad integridad y criticidad.
A.7.2.1	Directrices de clasificación.	0	No existe	0%	
A.7.2.2	Etiquetado	1	Etapa inicial	10%	
A.8	**SEGURIDAD A LOS RECURSOS HUMANOS**	1.7	Etapa Inicial	10%	
A.8.1	**Antes del empleo**	2.0	Etapa media	50%	
A.8.1.1	Funciones y responsabilidades	3	Definido	90%	
A.8.1.2	Investigación de Antecedentes	0	No Existe	0%	
A.8.1.3	Términos y condiciones de contratación	3	Definido	90%	
A.8.2	**Durante el empleo**	2.0	Etapa Media	50%	
A.8.2.1	Responsabilidades de la dirección	3	Definido	90%	
A.8.2.2	Capacitación en seguridad de la información.	0	No existe	0%	
A.8.2.3	Proceso disciplinario	3	Definido	90%	
A.8.3	**Cese de empleo**	1.0	Etapa Inicial	10%	
A.8.3.1	Responsabilidad de cese o cambio de empleo	0	No existe	0%	
A.8.3.2	Devolución de activos	1	Etapa inicial	10%	
A.8.3.3	Retirada de los derechos de acceso	2	Etapa media	50%	
A.9	**SEGURIDAD FISICA Y DEL ENTORNO**	1.2	Etapa Inicial	10%	
A.9.1	**Áreas seguras**	1.0	Etapa inicial	10%	
A.9.1.1	Controles de entrada	0	No existe	0%	
A.9.1.2	Seguridad de Oficinas	1	Etapa inicial	10%	
A.9.1.3	Protección contra las amenazas externas y de origen ambiental	0	No existe	0%	No existe ninguna protección contra amenazas de origen ambiental
A.9.1.4	Trabajo en áreas seguras	1	Etapa inicial	10%	
A.9.2	**Seguridad de los Equipos de tecnología**	1.3	Etapa inicial	10%	
A.9.2.1	Seguridad del cableado	2	Etapa media	50%	
A.9.2.2	Seguridad de los equipos fuera de las instalaciones	0	No existe	0%	

A.9.2.3	Reutilización o retirada de los equipos	2	Etapa media	50%	
A.10	**GESTION DE COMUNICACIONES Y OPERACIONES**	1.0	Etapa inicial	10%	
A.10.1	**Protección contra códigos Maliciosos.**	0	No existe	0%	**Control:** Certificar que la información este protegida contra códigos maliciosos. **Control:** Implementar controles de seguridad dirigidos por el área TIC en contra de códigos maliciosos.
A.10.1.1	Controles contra códigos maliciosos	0	No tiene	0%	
A.10.2	**Copias de Seguridad**	1	Etapa Inicial	10%	**Objetivo:** Proteger la información de pérdidas. **Control:** Realizar copias de seguridad a los activos de información según lo estipulado en el plan de respaldo de información.
A.10.2.1	Copias de seguridad de la información.	1	Etapa inicial	**10%**	Se realizan copias de seguridad cuando el usuario lo solicite, no hay un cronograma definido para las copias de seguridad.
A.11	**CONTROL DE ACCESO**	0,3	No existe	0%	
A.11.1	**Requisitos de negocio para el control de acceso**	0,0	No existe	0%	
A.11.1.1	Política de control de acceso	0	No existe	0%	
A.11.2	**Gestión de acceso de usuarios**	**1,0**	**Etapa inicial**	**10%**	
A.11.2.1	Registro de usuarios	1	Etapa inicial	10%	
A.11.2.2	Gestión de privilegios	0	No existe	0%	
A.11.2.3	Gestión de contraseñas de usuarios	1	Etapa inicial	10%	
A.11.3	**Responsabilidades de usuarios**	**0,5**	**No existe**	**0%**	
A.11.3.1	Uso de contraseñas	1	Etapa inicial	10%	
A.11.3.2	Política de puesto de trabajo despejado y pantalla limpia	0	No existe	0%	

A.11.4	**Control de acceso a la red**	**0,0**	**No existe**	**0%**	
A.11.4.1	Política de uso de los servicios de red	0	No existe	0%	
A.11.4.2	Control de conexión a la red	0	No existe	0%	
A.11.5	**Control de acceso al sistema operativo**	**0,0**	**No existe**	**0%**	
A.11.5.1	Procedimiento seguro de inicio de sección	0	No existe	0%	
A.11.5.2	Identificación y autenticación de usuarios	0	No existe	0%	
A.12	**ADQUISICIÒN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÒN.**	0	No existe		
A.12.1	**Controles Criptográficos.**	0%	No existe	0%	
A.12.1.1	Política del uso de los controles criptográficos.	0	No existe	0%	
A.12.1.2	Gestión clave	0	No existe	0%	
A.13	**GESTION DE INCIDENTES EN LA SEGURIDA DE LA INFORMACIÒN.**	0%	No existe	0%	
A.13.1	**Notificación de eventos**	0%	No existe	0%	
A.13.1.1	Notificación de eventos de seguridad de la información	0	No existe	0%	
A.13.1.2	notificación de puntos débiles	0	No existe	0%	
A.13.2	**Gestión de incidentes**	0%	No existe	0%	
A.13.2.1	Responsabilidades y procedimientos	0	No existe	0%	
A.13.2.2	Aprendizaje de los incidentes de seguridad.	0	No existe	0%	
A.13.2.3	Recopilación de evidencias.	0	No existe	0%	
A.14	**GESTION DE LA CONTINUIDAD DEL NEGOCIO.**	0,5%	No tiene	0%	
A.14.1	**Aspecto de la seguridad de la información**	0	No tiene	0%	
A.14.1.1	Continuidad del negocio y evaluación de riesgos.	1	Etapa inicial	10%	
A.15	**CUMPLIMIENTO**	1%	Etapa inicial	10%	
A.15.1	**Cumplimiento de las políticas**	0%	No existe	0%	
A.15.1.1	Cumplimiento de las políticas de seguridad	0	No existe	0%	

A.15.1.2	comprobación de cumplimiento técnico	0	No existe	0%	
A.15.2	**Auditorias de los sistemas de información**	3,0	Definido	90%	
A.15.2.1	Controles de auditoría de los sistemas de información	3	Definido	90%	
A.16	**RELACION CON LOS PROVEEDORES**	0%	No existe	0%	
A.16.1	Seguridad con los proveedores	0%	No existe	0%	
A.16.2	Gestión de servicios externos.	0%	No existe	0%	

Es importante resaltar, que algunos controles no están siendo ejecutados en el Instituto de Investigaciones Ambientales del Pacifico para que sean evaluados y socializados por la alta gerencia y el área de las TIC.

Los controles son los siguientes:

- A.7 Gestión de Activos
- A.11 Control de acceso
- A.12 adquisición desarrollo y mantenimiento de sistemas de información
- A.13 Gestión de incidentes
- A.14 Gestión de la continuidad del negocio
- A.15 Cumplimiento
- A.16 relación con los proveedores.

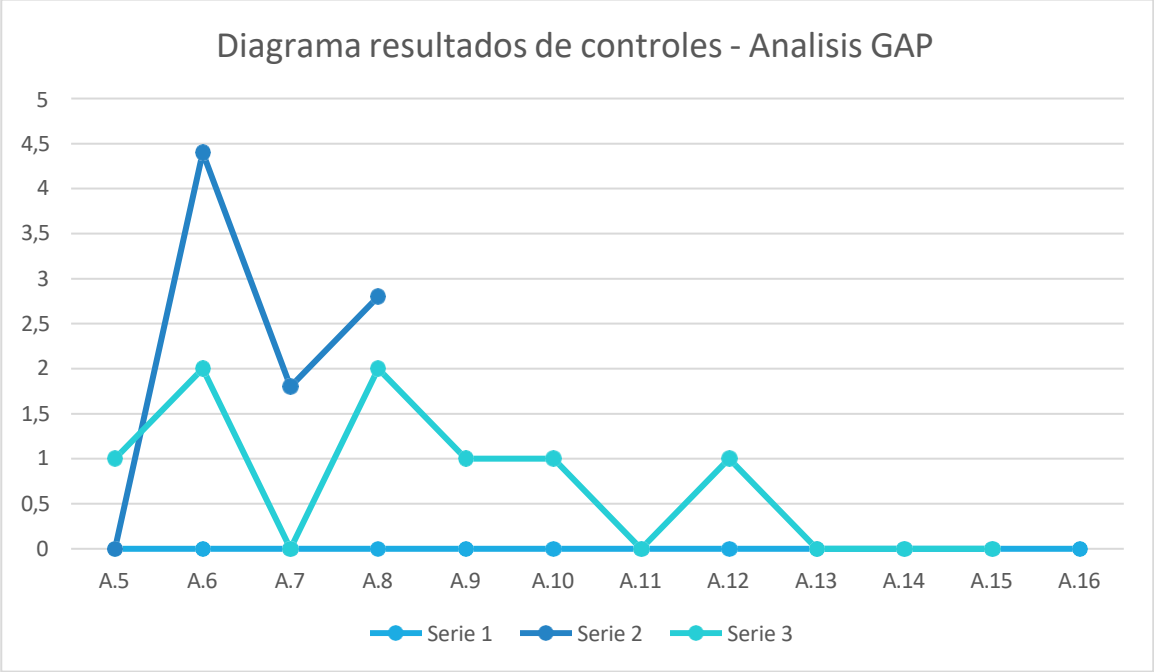
Análisis de Brecha. Se identifico el estado actual de la entidad en cuanto a la gestión de riesgo basa en la norma ISO 27001 anexo A entre dominios y controles para ser medidos dentro del análisis GAP en cumplimiento, estado y porcentaje.

Resultados del análisis brecha o GAP de acuerdo con los dominios y controles ISO/IE 27002:2005.

Dominio	Cumplimiento	Estado	Porcentaje
A.5 Políticas de Seguridad	1,0	Etapa inicial	10%
A.6 Aspectos organizativos de la seguridad de la información.	5,0	Etapa media	50%
A.7 Gestión de activos	0.0	No existe	0%

A.8 Seguridad ligada a los recursos humanos	5,0	Etapa media	50%
A.9 Seguridad física y del entorno	1,0	Etapa inicial	10%
A.10 Gestión de comunicaciones y operaciones.	1,0	Etapa inicial	10%
A.11 Control de acceso	0,0	No existe	0%
A.12 Adquisición, desarrollo y mantenimiento de sistemas de información	1,0	Etapa inicial	10%
A.13 Gestión de incidentes de la seguridad de la información	0,0	Etapa inicial	10%
A.14 Gestión de la continuidad del negocio	0,0	Etapa inicial	10%
A.15 Cumplimiento	0,0	Etapa inicial	10%
A.16 Relación con los proveedores	0,0	Etapa inicial	10%

El resultado de los controles y dominios de acuerdo con la valoración y el cumplimiento también se puede representar en una gráfica, como se muestra a continuación:



8. PROPONER LAS POLITICAS DE SEGURIDAD INFORMÁTICA CON LAS ACCIONES DE GESTIÓN, LOS RECURSOS, RESPONSABLES, PRIORIDADES PARA MANEJAR LOS RIESGOS DE SEGURIDAD DE LA INFORMACION PARA EL INSTITUTO DE INVESTIGACIONES AMBIENTALES DEL PACIFICO JOHN VON NEUMANN

8.1. POLÍTICAS DE SEGURIDAD INFORMÁTICA.

“Constituye el documento fundamental para el control y la seguridad en la explotación de las tecnologías informáticas donde las medidas que se establecen son de obligatorio cumplimiento para todo el personal que haga uso de las tecnologías informáticas instaladas en la institución.”[23]

Con estas políticas se determina el cumplimiento de los controles que están etapa no existente, en etapa inicial y etapa media para llegar a un estado de cumplimiento definido. Esto se logra mediante la gestión de los recursos, definición de roles y responsabilidades, definición de los riesgos y vulnerabilidades y el manejo de la seguridad de la información.

[23] EcuRed. Obtenido de EcuRed.

Para ello se proponen políticas de seguridad de acuerdo con el resultado de las encuestas, detalles de dominios y controles, análisis de la seguridad de la información y análisis brecha

Nombre	Políticas de capacitación sobre seguridad de la información
Objetivo	Capacitar al personal sobre seguridad de la información
Responsable	Personal del área TIC
Actividades	Capacitación sobre la seguridad de la información y los riesgos a lo que se expone. Talleres aplicativos sobre la identificación de activos, riesgos, vulnerabilidades y comunicación de incidentes
A quien va dirigido	Personal del IIAP

Políticas para tratar riesgo:

CUADRO 5. Política de respuesta a incidentes de seguridad informática

CUADRO 6. Políticas de capacitación sobre seguridad de la información

Nombre	Política de Gestión de vulnerabilidades
Objetivo	Advertir el aprovechamiento de las vulnerabilidades
Responsable	Personal del área TIC
Actividades	Definir roles y actividades Definir los recursos que se deben utilizar para la mitigación Tomar acciones en cuanto a las vulnerabilidades Definir el procedimiento a seguir una vez identificada la vulnerabilidad
Nombre	Política de respuesta a incidentes de seguridad informática.
Objetivo	Proceder de forma acertada ante la identificación de incidentes de seguridad informática.
Responsable	Personal del área TIC
Actividades	Definir responsables y actividades Establecer procedimiento para la planificación y preparación de respuestas a incidentes. Establecer procedimientos frente a la valoración y toma de decisiones sobre eventualidades de seguridad. Comunicar los incidentes a la alta gerencia si es el caso.

CUADRO 7. Política de Gestión de vulnerabilidades

CUADRO 8. Política de control de acceso

Nombre del Plan	Política de control de acceso
Objetivo	Controlar los derechos de acceso de los usuarios
Responsable	Personal del área TIC
Actividades	Definir políticas de control de acceso Registro de usuarios Definir políticas de privilegios de acceso Comunicar si ocurre una suplantación de usuario

CUADRO 9. Política del uso aceptable de los activos

Nombre del Plan	Política del uso aceptable de los activos
Objetivo	Identificar los activos con su respectiva clasificación, propietario o custodio y responsabilidades
Responsable	Personal del área TIC
Actividades	Realizar inventario de activos y definir políticas

8.1.1. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Responsables: Personal Área TIC
Objetivo: Resguardar la información del instituto de Investigaciones Ambientales del Pacifico.
Recursos: Utilizar la metodología Magerit y el análisis de los puertos.

En ninguna circunstancia se debe divulgar la información clasificada de cada área o de la institución en general clasificada como confidencial a personas terceras no autorizadas. Esta política o reglas se debe cumplir, aun así, ya no esté vinculado a la institución.

Es de suma importancia que todos los activos de la información tengan un propietario quien se encarga de proteger la información. al mismo tiempo, velar por el cumplimiento de la disponibilidad, confidencialidad e integridad de la misma.

Todo empleado del Instituto de Investigaciones Ambientales del Pacifico deben recibir una capacitación y actualización sobre seguridad y privacidad de la información. en la cual se debe dar a conocer los requerimientos de seguridad y responsabilidades. también, el uso adecuado de los recursos tecnológicos dados por la institución para el buen desempeño de sus actividades

Recomendaciones:

- Realizar respaldo o backup de la información un periodo determinado.
- No abrir documentos adjuntos de correos electrónicos de dudosa procedencia
- No visitar páginas que no sea seguras o contengan contenido inapropiado
- En cuanto a las contraseñas, procurar no utilizar la misma para varias cuentas en plataformas o sistemas de información.
- Controlar los privilegios de acceso a sistemas de información
- Evitar ocupar memoria en archivos personales, debido que esto puede traer complicaciones en el buen funcionamiento del equipo
- Utilizar el correo electrónico de la empresa para recibir y enviar documentos solamente de la entidad.
- No Divulgar la información confidencial a terceros
- Evitar al máximo darles mal uso a los equipos de cómputos.
- Darle Priorizar y analizar los recursos informáticos de la empresa
- Tener un plan que determine copias de seguridad, validación de empleados, integridad en los datos importantes,
- Control de acceso a los sistemas de información y equipos de computo
- Mantener actualizados los sistemas operativos, los sistemas de información en cuanto a seguridad, firewall para evitar que sean vulnerados

Finalmente, dentro del análisis de los controles se debe tener en cuenta al dueño del riesgo (dueño del proceso), ya que es el resultado de los análisis realizados a través del seguimiento y aplicación de los pasos descritos anteriormente en el tratamiento del riesgo y los cuales deben tener el concurso de todos los interesados.

8.1.2. POLÍTICA DEL BUEN USO DE LOS RECURSOS TECNOLÓGICOS

Objetivo: Establecer el buen uso de los recursos tecnológicos.
Responsables: Personal Área TIC
Recursos: Formato hoja de vida de equipos

El Instituto de Investigaciones Ambientales del Pacifico, asigna los recursos tecnológicos como herramientas de trabajo para el buen desempeño laboral
Cada equipo de cómputo está configurado con lo necesario para su funcionamiento:

- Sistema operativo: Windows

- Office (Acces, Excel, OneNote, One Drive, Outlook, Power Point,
- Publisher, Word.)
- WinRAR
- Nitro PDF
- Antivirus
- Skype

Es de importancia resaltar que la instalación de software se encuentra bajo la responsabilidad del área de Tecnología y Sistemas de Información, por tanto, son los autorizados para realizar esta actividad. Toda solicitud debe realizarse por medio del formato llamado Solicitud de Soporte anexados al Manual de Calidad del Instituto. Además, Ningún empleado debe realizar cambios relacionados con la configuración de los equipos.

Los empleados del instituto son responsables de hacer buen uso de los recursos tecnológicos. En ninguna circunstancia deben ser utilizados para beneficio propio, realizar actividades ilícitas o mal intencionadas que atenten contra otros.

Todo activo tecnológico debe ser entregado al finalizar contrato laboral de forma definitiva Esto incluye los documentos corporativos, equipos de cómputo (Hardware y Software), carnet información institucional que tenga almacenada en los equipos de cómputo. Si un equipo de cómputo requiere formateo o reinstalación de aplicaciones por virus u otro daño debe realizar una solicitud de soporte técnico a través de los formularios que están anexados al Manual de calidad.

El empleado, no deberá abrir los equipos de cómputo, sacar o cambiar componentes de estos.
Si el equipo de cómputo presenta fallas o mal funcionamiento, el responsable del equipo debe reportar lo sucedido al área de Tecnología y Sistemas de Información, Adicional, se hará una evaluación del equipo para determinar el tipo de daño y la reparación que se requiere.

Al entregar el equipo de cómputo se deberá diligenciar un acta donde evidencie la entrega del equipo. El personal del área Tecnología y Sistemas de Información debe corroborar la información del equipo en el formato Hoja de vida de los computadores.

En caso de que un equipo de cómputo o impresoras sea hurtado o extraviado, el empleado deberá reportarlo al área de Tecnología y Sistemas de información. Si es robo deberá presentar también la denuncia respectiva.

8.1.3. POLÍTICA DE BACKUP

Objetivo: Establecer medios de respaldo de información para asegurar la información.
Responsable: Personal área TIC
Recursos: Disco Nas

El Área de Tecnologías de la Información y las Comunicaciones, son los responsables de la seguridad de la información en compañía de los propietarios de la misma para juntos seleccionar la información de carácter urgente que se le debe aplicar la copia de seguridad y con qué frecuencia se debe realizar. Para ello, se debe elaborar y mantener el inventario de activos de la información.

Se debe definir y documentar un esquema de respaldo de la información.
Los encargados del área de Tecnología de la Información y las Comunicaciones son los responsables de:

Establecer el periodo de retención de la información

El sitio alterno donde se almacenan las copias de seguridad debe para cumplir con las medidas de protección y seguridad física

Guardar los medios de almacenamiento de información en un ambiente que cuente con las instrucciones específicas puestas por los fabricantes.

Crear un cronograma para darle fecha exacta a cada uno de los usuarios. Si el usuario requiere cambio de fecha debe avisar con dos días de anticipación para reprogramar la copia de seguridad.

8.1.4. POLÍTICAS DEL BUEN USO DE INTERNET

Objetivo: Establecer reglas sobre el buen uso del internet, con el objetivo de asegurar una apropiada protección de la información del Instituto de Investigaciones Ambientales del Pacifico.
Responsables: Personal área TIC
Recursos: Clave para el acceso a internet

Los usuarios autorizados para hacer uso del servicio de Internet son responsables de evitar prácticas o usos que puedan comprometer los recursos tecnológicos de la del Instituto que afecte la seguridad de la información.

Todos los usuarios que se encuentren autorizados deben de dar un uso razonable y bajo ninguna razón pueden utilizar el servicio para realizar prácticas ilegales o mal intencionadas que atenten contra las políticas de seguridad de la información.
Evitar el envío o descarga de información de un tamaño grande o pesado que pueda congestionar la red a menos que sea algo para el buen desempeño de la actividad laboral.

Personas externas a la institución que requieran acceso a internet realizarlo por medio de la red WIFI y pedir la contraseña al equipo de sistemas y cumplir con los requisitos una vez que tengan acceso al servicio de internet.
No se permite el acceso a páginas con contenido de pornografía, actividades criminales, hacking, discriminación, contenido malicioso, suplantación de identidad, spyware y páginas de alto riesgo.

Para controlar el buen uso del internet en la entidad se implementa la utilidad del proxy web el cual ayuda al control de la red, media el protocolo HTTP para la gestión correcta de acceso a diferentes sitios trabajados en ese protocolo.

Con el proxy web, el responsable de la seguridad en el área de las TIC administra el acceso a la red teniendo como resultado del consumo, navegación, tiempo, los sitios más visitados y evaluación de riesgo de los sitios.

9. CONCLUSIONES

El diseño de un sistema de seguridad, prevención y gestión del riesgo bajo el contexto de la norma ISO 27001, tiene como objeto minimizar los ataques cibernéticos y la complejidad en que se encuentra la seguridad de la información. Este sistema incorpora herramientas expuestas por la normatividad ISO 27001 en cuanto a la confidencialidad, integridad y disponibilidad de la información.

En el presente proyecto se describe la importancia de la gestión del riesgo que se presentan en la seguridad de la información, los estándares y metodología para el desarrollo del análisis de vulnerabilidades en la entidad como la ISO 27001, Magerit, y escaneo de vulnerabilidades con la herramienta OWASP ZAP versión 2.11.

Todas las metodologías y normas mencionadas en este proyecto permitieron realizar un análisis evaluativo en referencia a los activos, amenazas, controles y procedimientos para finalmente obtener un tratamiento efectivo de los riesgos y vulnerabilidades de acuerdo con la ISO 27001 cuyo objeto sea la protección de los activos y recursos de la información.

La dificultad de la inseguridad informática no solamente se trata de identificar los riesgos, es también mantener en constante actualización todas las herramientas que ayuden a minimizar los ataques, la disponibilidad del personal de seguridad, los reporte o alertas de todos los casos posibles de riesgo, el continuo desarrollo de nuevas aptitudes y ética profesional.

Un Sistema de Gestión de Seguridad de la Información no se implementa por llenar requisitos, al contrario, se implementa buscando objetivos que agreguen valía a la organización. También, determinar los activos de información, los riesgos y fallas de seguridad que están presentes en la infraestructura tecnológica del Instituto de Investigaciones Ambientales del Pacifico.

Una vez se realiza la evaluación y análisis de riesgo, la entidad tiene una herramienta clave para el tratamiento de vulnerabilidades, diagnóstico sobre el estado de seguridad informática y activos de información. En base a la evaluación es posible actualizar o tener en cuenta las políticas que ayudan a la corrección de vulnerabilidades detectados y la gestión de seguridad a lo largo del tiempo, para corroborar y avalar que las vulnerabilidades encontradas anteriormente no sean un

problema o generen más dificultad para el desarrollo de las actividades, investigación, misión y visión de la institución.

10. RECOMENDACIONES

De acuerdo con el estudio realizado sobre la seguridad de los activos de información del Instituto de Investigaciones Ambientales del Pacifico teniendo en cuenta la norma ISO 27001 buscando minimizar los ataques cibernéticos se hacen las siguientes recomendaciones:

- **Roles y Responsabilidades.**

Es necesario establecer permisos de acceso a los usuarios a los diferentes sistemas de información o equipos de cómputos de la entidad para así controlar el abuso de privilegios y evitar violar la integridad de la información. Los que tengan permiso de acceder a dicha información privada debe estar informado de forma precisa de sus funciones y obligaciones en el tratamiento de los datos.

- **Establecer medidas de seguridad.**

Capacitar al personal de Jurídica y TIC en todas las leyes que acobijan el tratamiento de la información para así mismo hacer cumplir las sanciones que se deben implementar siempre y cuando haya incumplimiento y abuso de privilegios.

- **Comunicación con terceros:**

Servidores, páginas web y demás servicios son los que la entidad puede contratar. Al realizar esta acción de contratación de servicios es necesario dar a conocer a terceros las políticas de seguridad y las sanciones de la entidad para que puedan garantizar un buen servicio. El no informar las políticas a terceros pueden incurrir en acciones que perjudiquen los activos de información de la entidad y colocando en riesgo la disponibilidad, integridad y confidencialidad.

Capacitar y concientizar a todo el personal del Instituto de Investigaciones Ambientales del Pacifico, generar interés, participación y compromiso es fundamental para garantizar la seguridad de la información, prevención y gestión del riesgo.

Evitar los abusos de privilegios, colocar contraseñas a todos los equipos, restringir las descargar por los usuarios.
Poner en marcha el plan de mantenimiento preventivo y correctivo definido por el área TIC para así evitar daños que paralicen las actividades que sean de mayor peso para el desarrollo de la Institución

11. BIBLIOGRAFÍA

AGUIRRE, J. Introducción a la seguridad informática y criptografía clásica. Algoritmo de cifra clásica. 2016.

AMAYA, Y. Norma técnica NTC ISO-IEC Colombiana 27001. 2006.

BLOG ESPECIALIZADO EN SISTEMA DE GESTION DE SEGURIDAD INFORMATICA. Componentes de los sistemas de gestión de seguridad de la información. 2020.

CAMACHO, M. Esteganografía. El arte de camuflar archivos. 2013.

CAMELO, L. Seguridad de la Información en Colombia. Colombia: Marco legal de Seguridad de la Información. 2010.

CAURIN, J. Emprende Pyme. Políticas de Seguridad. 2018. LEY 1273 DE 2009. Colombia. 2020.

BREVE HISTORIA DE LA SEGURIDAD INFORMATICA. 2019. UNIDAD DE INFORMATICA. Colombia: UIFCE.

COMPUTERWORLD. Nueva tendencia esencial en seguridad. 2018.

CONCEPTOS DE SEGURIDAD. Conceptos de Seguridad.

CONEXIONESSAN. Cuatro pasos para implementar un Sistema de Seguridad de Información. 2019.

CORONEL, J., & MARTINEZ, J. E. Criptografía. 2019

CRESPO, A. Redes Zone. 2017

DE LUZ, S. Nmap: Descarga, instalación y manual de uso paso a paso. 2009. DELSOL, S. Las políticas de empresa y su importancia. 2019.

ECHEVERRY, F. (s.f.). Inicio y evolución de la seguridad informática en el mundo. Colombia: Universidad Piloto Colombia.

EUGENE SPAFFORD. y JAMES P. ANDERSON. Un pionero en seguridad de la información. Security&privacy, 2008. 9 Vol. 6.

EXCELLENCE, I. SGSI. Los tres pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad. 2018.

FRANCISCONI.ORG. Soluciones informáticas. 2014. GCFA.
Aprende Libre. *Informática Básica*. 2014

INCIBE. DMZ y cómo te puede ayudar a proteger tu empresa. 2019. INCIBE.
Glosario de términos de ciberseguridad.

INSTITUTO COLOMBIANO DE NORMAS TECNICAS. Norma técnica NTC NTC ISO/IEC 27001. Colombiana, 2006.

INSTITUTO DE INVESTIGACIONES AMBIENTALES DEL PACIFICO. Pacifico, I. d. Nosotros

INSTITUTO NACIONAL DE ESTANDARES Y TECNOLOGIA. 2019.

JYCELL-NUMAEL. Seguridad Informática. Historia de la seguridad informática. 2017.

LAS TIC. Seguridad en Redes.

LEY ESTATUTARIA 1266 DE 2008. Colombia, 2020.

MARTINEZ, M. y GERALDIN, B. *¿Qué es el cifrado y para qué sirve?*. 2017

MINISTERIO DE JUSTICIA. *Sistema Único de información normativa.* 2014

MINISTERIO DE TECNOLOGIA DE LA INFORMACION Y COMUNICACIONES.

Modelo de Seguridad y privacidad de la información. 2016.

---------- --. Controles de seguridad y privacidad de la información. 2016

--------. Guia de Mejora Continua. 2015.

--------. Controles de Seguridad y privacidad de la información. 2016.

--------. Controles de Seguridad y privacidad de la información. 2016.

--------. Guía de gestión de riesgo. Seguridad y privacidad de la información. 2018.

--------. Procedimientos De Seguridad. Seguridad y privacidad de la información. 2016.

--------. -------- Seguridad y privacidad de la información. 2016.

--------. -------- Seguridad y privacidad de la información. Obtenido de Guía de

Gestión de Riesgo. versión 2016.

---------- -. Sistema de gestión de seguridad de la información. 2018.

--------. Confidencialidad. 2020.

MODELO DE SEGURIDAD. Fortalecimiento de la gestión. 2018.

PLAN DE SEGURIDAD PARA TU EMPRESA. 5 elementos indispensables. ¿Qué es un plan de seguridad y cómo puede ayudar a tu empresa? 2018.

RAFFINO, M. E. *Concepto de* software. 2020.

RAMIREZ, J. C. Metodología para la elaboración del plan de seguridad informática. *2020.*

ROUSE, M. Copia de Seguridad o Respaldo.

SIGNIFICADOS. Significado de vulnerabilidad. 2018.

--------. Significado de Seguridad Informática. 2019 GLOSARIO DE SEGURIDAD. *Glosario de seguridad. 2006* TECNOLOGIA –

INFORMATICA. Que es la Criptografía. 2020. THOMPSON. Que es Información. 2010.

UNIVERSIDAD TECNOLOGICA DEL CHOCO. Historia del IIAP.

CORDOBA, B. Y. Diseño de un sistema de gestión de seguridad de la información con base en la gestión de riesgos. 2021

12. ANEXOS

ANEXO A.

TERMINOS DE REFERENCIA PARA CONTRATISTA IIAP

https://docs.google.com/document/d/1tkOHCllq1zvxQaQMlSgKpQwGQxeAGyHE/edit?usp=sharing&ouid=103062890683831167422&rtpof=true&sd=true

ANEXO B.

GUIA SEGURIDAD DIGITAL

https://docs.google.com/document/d/1vE1MhH22_8O36IKAuYtftUfWIDMrOi-t/edit?usp=sharing&ouid=103062890683831167422&rtpof=true&sd=true

ANEXO C.

MATRIZ DE INVENTARIO Y CLASIFICACION DE ACTIVOS

https://drive.google.com/drive/folders/1Ru0kih9r1-Cs74ciPsNWU4SlG8tUay9x?usp=share_link

ANEXO D.

GUIA DE INVENTARIO Y CLASIFICACION DE ACTIVOS

https://docs.google.com/document/d/1v521x2Peym1mKZdyb2PcVWYABLI4Kxzf/edit?usp=sharing&ouid=103062890683831167422&rtpof=true&sd=true

ANEXO E.

ENLACE DEL VIDEO

https://youtu.be/MH_V8qgyFLI

ANEXO F.

BITACORA DE COPIAS DE SEGURIDAD.

https://docs.google.com/spreadsheets/d/1qJQ4LyezDsQdiNYpcXnHmFGlZFyD4x5pwG4NtUVEf8Q/edit#gid=1739928432

ANEXO G.

INVENTARIO IIAP

https://docs.google.com/spreadsheets/d/1gQKn_GqsLtCDRDZ0UsBZBquAxoz6m0D5/edit?usp=share_link&ouid=103062890683831167422&rtpof=true&sd=true

ANEXO H.

RESULTADOS ENCUESTA

https://docs.google.com/document/d/1LUk_G11EoEJxzkswl2GC5Fg_BV9hvoUC/edit?usp=share_link&ouid=103062890683831167422&rtpof=true&sd=true