DISEÑO DE LA ETAPA DE PLANIFICACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN EL PROCESO DE GESTIÓN DE RECURSOS FÍSICOS Y TECNOLÓGICOS DE LA EPS INDÍGENA MALLAMAS

CRISTHIAN BARNY PORTILLA MARTÍNEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
IPIALES - NARIÑO
2021

DISEÑO DE LA ETAPA DE PLANIFICACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN EL PROCESO DE GESTIÓN DE RECURSOS FÍSICOS Y TECNOLÓGICOS DE LA EPS INDÍGENA MALLAMAS

CRISTHIAN BARNY PORTILLA MARTÍNEZ

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

HERNANDO JOSÉ PEÑA
Director de Trabajo de Grado

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
IPIALES - NARIÑO
2021

NOTA DE ACEPTACIÓN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ipiales., 28 de Noviembre 2021

DEDICATORIA

Dedico este proyecto, a Dios primeramente por permitirme la vida y la salud, en estos tiempos difíciles que atravesamos a nivel mundial, que me permitió realizar uno más de mis logros como profesional.

A mi esposa por su apoyo incondicional e inmenso amor, que siempre estuvo ahí, para no desfallecer, ante las circunstancias difíciles de mi entorno laboral y profesional.

A mis hijos que son la fuente de mi inspiración y quienes comprendieron, que mis logros son para brindarles un futuro mejor para todos, en donde tuve que sacrificar tiempo que dejé de compartir con ellos, pero siempre me apoyaron y me llenaron con su amor.

AGRADECIMIENTOS

Mis agradecimientos especiales al Dr. Fabio Enríquez Miranda, Gerente de la Empresa MALLAMAS, que me permitió desarrollar este proyecto en tan prestigiosa empresa, al igual que a todos los colaboradores que me apoyaron con su tiempo y profesionalismo.

A la Universidad UNAD, por brindarme a través de los tutores y directores, grandes aprendizajes, en cada uno de los temas del currículo académico.

A mi familia, por su gran apoyo y cariño en todos los momentos a lo largo de esta experiencia profesional.

CONTENIDO

Pág.

INTRODUCCIÓN 21

1.1 FORMULACIÓN DEL PROBLEMA 23

2 JUSTIFICACIÓN 24

3 OBJETIVOS 25

3.1 OBJETIVOS GENERAL 25

3.2 OBJETIVOS ESPECÍFICOS 25

4 MARCO REFERENCIAL 26

4.1 MARCO TEÓRICO 26

4.1.1 Sistema de gestión de seguridad de la información 26

4.1.1.1 La importancia de un SGSI 26

4.1.2 Metodología de gestión 28

4.1.3 El modelo de seguridad y privacidad de la información – MSPI 30

4.2 MARCO CONCEPTUAL 30

4.3 MARCO CONTEXTUAL 32

4.3.1 Reseña histórica de la EPS MALLAMAS 32

4.3.2 Misión 34

4.3.3 Visión 34

4.3.4 Mapa de procesos 34

4.3.5 Procedimientos del proceso de Gestión de Recursos Físicos y tecnológicos. 35

4.4 MARCO LEGAL 35

5.1 Técnicas de recolección de información 39

5.2 Población 40

5.3 Muestra 40

6 DIAGNOSTICO DE SEGURIDAD DE LA INFORMACIÓN 41

6.1 CONTEXTO DE LA ENTIDAD 41

6.1.1 Levantamiento de la Información 42

7 INVENTARIO DE ACTIVOS 50

7.1.1 Activos 50

7.1.2 Proceso de estudio 51

7.1.2.1 Tipos de activos 51

7.1.3 Inventario de Activos de MALLAMAS EPS INDÍGENA 53

7.1.3.1 Dimensionar la Valoración 55

7.1.3.2 Criterios de Valoración Cuantitativa 55

7.1.3.3 Criterios de Valoración Cuantitativos 57

7.1.4 Identificación y valoración de amenazas 62

7.1.4.1 Amenazas 62

7.1.4.2 Identificar las Amenazas 62

7.1.4.3 Valorar las amenazas 65

7.1.5 Determinar el riesgo potencial 68

8 CONTROLES A LOS RIESGOS DE SEGURIDAD 80

8.1 controles a los riesgos por activos 80

8.2 plan de ACCIÓN de los controles a implementar 80

9 POLÍTICAS DE SEGURIDAD DE INFORMACIÓN 158

9.1 Política general de seguridad de la información. 158

9.1.1 Objetivo 160

9.1.2 Alcance 160

9.2 Política de Control de Acceso 162

9.2.1 Objetivo 162

9.2.2 Alcance 162

9.2.3 Criterios 162
9.3 Política de Acceso a redes y Servicios de red 164
9.3.1 Objetivo 164
9.3.2 Alcance 164
9.3.3 Criterios 164
9.4 Política de ESCRITORIO Y PANTALLA LIMPIOS 166
9.4.1 Objetivo 166
9.4.2 Alcance 167
9.4.3 Criterios 167
9.5 POLÍTICA DE USO DE LOS ACTIVOS 169
9.5.1 Objetivo 169
9.5.2 Alcance 169
9.5.3 Criterios 169
9.6 POLÍTICA DE PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS 172
9.6.1 Objetivo 172
9.6.2 Alcance 172
9.6.3 Criterios 173
□ Controles contra código malicioso 173
9.7 POLÍTICA PARA EJECUTAR COPIAS DE SEGURIDAD 175
9.7.1 Objetivo 175
9.7.2 Alcance 175
9.7.3 Criterios 175
9.8 POLÍTICA PARA LA TRANSFERENCIA DE INFORMACIÓN 177
9.8.1 Objetivo 177
9.8.2 Alcance 177
9.8.3 Criterios 177
9.9 POLÍTICA DE SEGURIDAD PARA RELACIÓN CON PROVEEDORES 178
9.9.1 Objetivo 178
9.9.2 Alcance 178

9.9.3 Criterios 178
9.10 POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES 179
9.10.1 Objetivo 179
9.10.2 Alcance 179
9.10.3 Criterios 180
9.10.3.1 Modo en que se utiliza la información 180
9.10.3.2 Derechos de los titulares de los datos personales 180

CONCLUSIONES 182
RECOMENDACIONES 184
BIBLIOGRAFÍA 185
ANEXOS 189

LISTA DE TABLAS

Pág.

Tabla 1 Evaluación de efectividad de controles 43
Tabla 2. Avance PHVA 45
Tabla 3. Rangos de calificación 46
Tabla 4 Valoración de probabilidad y degradación 65

LISTA DE FIGURAS

Pág.

Figura 1 Mapa de Procesos MALLAMAS EPS INDÍGENA 35
Figura 2 Desarrollo de la Metodología de Autodiagnóstico..... 42
Figura 3 Grafica avance PHVA 45
Figura 4: Escala valor activo Cuantitativa 57

LISTA DE CUADROS

pág.

Cuadro 1. Instrumentos de recolección de información 39
Cuadro 2. Procesos Gestión de Recursos Tecnológicos 51
Cuadro 3. Inventario Activos 53
Cuadro 4 Valoración del Activo Cuantitativo 56
Cuadro 5 Valoración de activos 58
Cuadro 6 Valoración de los activos en escala C.C 61
Cuadro 7 Valoración de la probabilidad 66
Cuadro 8 Calculo del Riesgo 69
Cuadro 9 Valoración de la Criticidad 73
Cuadro 10 Plan de acción para llevar a cabo los controles ante los riesgos 81

LISTA DE ANEXOS

pág.
Anexo A Autorización de la Organización 189
Anexo B RAE 190

GLOSARIO

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

ACTIVO 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.

ARCHIVO: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)

AMENAZAS: 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).

AUTORIZACIÓN: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)

BASES DE DATOS PERSONALES: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)

CIBERSEGURIDAD: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701)

CONFIDENCIALIDAD. "Asegurar que solo quienes estén autorizados pueden acceder a la información."[1]

DISPONIBILIDAD. Asegurar que los usuarios autorizados tengan acceso a la información y a sus activos asociados cuando lo requieran.

CONTROL: Medios para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal.

EVALUACIÓN DE RIESGOS. Todo proceso de análisis y valoración del riesgo. [ISO/IEC Guía 73:2002]

ESTÁNDAR: Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares son diseñados para promover la implementación de las políticas de alto nivel de la entidad antes de crear nuevas políticas

GESTIÓN DEL RIESGO. Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. [ISO/IEC Guía 73:2002]

---

1 Firma-e. Pilares de la Seguridad de la Información: confidencialidad, integridad y disponibilidad [Sitio web]. [Consulta: 26 de Marzo de 2021]. Disponible en: https://www.firma-e.com/blog/pilares-de-la-seguridad-de-la-informacion-confidencialidad-integridad-y-disponibilidad/

INTEGRIDAD. “Asegurar que la información y sus métodos de proceso son exactos y completos.” [2]

LEY DE HABEAS DATA: Se refiere a la Ley Estatutaria 1266 de 2008. • Ley de Transparencia y Acceso a la Información Pública: Se refiere a la Ley Estatutaria 1712 de 2014.

MEJOR PRÁCTICA: Una regla de seguridad específica o una plataforma que es aceptada, a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de los sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la entidad.

MECANISMOS DE PROTECCIÓN DE DATOS PERSONALES: Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.

PLAN DE CONTINUIDAD DEL NEGOCIO Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

---

[2] Firma-e. Pilares de la Seguridad de la Información: confidencialidad, integridad y disponibilidad [Sitio web]. [Consulta: 26 de Marzo de 2021]. Disponible en: https://www.firma-e.com/blog/pilares-de-la-seguridad-de-la-informacion-confidencialidad-integridad-y-disponibilidad/

PLAN DE TRATAMIENTO DE RIESGOS. Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

PRIVACIDAD. En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

POLÍTICA. Toda intención y directriz expresada formalmente por la Dirección.

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).

SEGURIDAD DE LA INFORMACIÓN. Preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no-repudio y confiabilidad pueden estar involucradas.

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).

TRATAMIENTO DEL RIESGO. Proceso de selección e implementación de medidas a para modificar el riesgo.

TRATAMIENTO DE DATOS PERSONALES: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

VALORACIÓN DEL RIESGO. Proceso de comparación del riesgo estimado frente a criterios de riesgo establecidos para determinar la importancia del riesgo. [ISO/IEC Guía 73:2002]

VULNERABILIDAD Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

RESUMEN

En el presente documento se documentara la realización de etapa de planificación de un sistema de gestión de seguridad en la información en el proceso de gestión de recursos físicos y tecnológicos, teniendo en cuenta que la empresa MALLAMAS EPS INDÍGENA, no dispone de un sistema de gestión de la información, que posibilite garantizar algunos de los principios básicos como, la integridad, confidencialidad y la disponibilidad, pese a que maneja información relevante y confidencial de todos sus procesos, la entidad cuenta con un área de TIC, la cual tienen a cargo el manejo de la infraestructura tecnología sin embargo esta no cuenta con el manejo de políticas de seguridad en la información, al igual un inventario de activos que permita una gestión de riesgo adecuada.

El diseño de este SGSI, en la EPS, conlleva a que todos los actores de la entidad se involucren, así mismo el compromiso de la alta gerencia, nos permitirá llevar a cabo esta planificación y posteriormente su implementación, de esta manera lograr un grado de madurez de seguridad óptimo.

Por este motivo se propone realizar el desarrollo del diseño de la fase de planificación de un sistema de gestión de información, la cual se realizará bajo el marco de la ISO/IEC 27001:2013, al igual con su guía de buenas prácticas enmarcadas en la ISO/IEC 27002:2013, que permitirá la adecuada gestión de los riesgos y establecer políticas de seguridad, que al final garantizará la integridad, confidencialidad y disponibilidad de la información.

ABSTRACT

This document will document the implementation of the planning stage of an information security management system in the process of managing physical and technological resources, taking into account that the company MALLAMAS EPS INDÍGENA does not have a management system of information, which makes it possible to guarantee some of the basic principles such as integrity, confidentiality, and availability, even though it handles relevant and confidential information of all its processes, the entity has an ICT area, which is in charge of the management of the technology infrastructure, however, it does not have the management of information security policies, as well as an inventory of assets that allows adequate risk management.

The design of this ISMS, in the EPS, implies that all the entity's actors are involved, as well as the commitment of senior management, which would allow us to carry out this planning and subsequently its implementation, in this way to achieve a degree of optimal security maturity.

For this reason, it is proposed to carry out the development of the design of the planning phase of an information management system, which will be carried out under the framework of ISO / IEC 27001: 2013, as well as its guide to good practices framed in the ISO / IEC 27002: 2013, which will allow adequate risk management and establish security policies, which in the end will guarantee the integrity, confidentiality, and availability of the information.

INTRODUCCIÓN

En la actualidad la globalización digital a traídos magníficos beneficios a las empresas, ya que pueden acceder a toda la información necesaria, con sus proveedores, clientes así mismo la interacción con los mismos a través de plataformas digitales, convirtiéndose la información como un activo importante para las empresas actualmente. Esto ha abierto una brecha importante para que los ciberdelincuentes obtengan esta información y sea utilizada para fines ilícitos.

Por este motivo las empresas, actualmente deben reconocer la importancia de salvaguardar la información de sus cliente y proveedores, aplicando cualquier tipo de estrategias o planes que permitan minimizar estas actuaciones, tratando de realizar un análisis para determinar los riesgos y como estos pueden ser minimizados, esto se logra a través de la planificación de sistemas de seguridad de la información, ya que estos tienen como pilares fundamentales la confidencialidad, disponibilidad e integridad de la información, los cuales se logran contando con procesos sistémicos, organizados y documentados, este tipo de sistemas garantiza que se conozcan los activos, que se definan los riesgos, los cuales se realizara unos planes de mitigación, con el propósito de minimizar o controlar los mismos.

Las entidades de salud, para este caso las EPS, manejan información importante de sus afiliados, sus proveedores y demás actores del sistema general de seguridad social en salud, esta información reposa en sistemas informáticos de la entidad, los cuales son administrados por las áreas de las TICS, las cuales velan en sus procesos tener a disposición esta información, por lo cual este proyecto se encuentra enfocado a que esta área de las TICS, a través de los estándares como la ISO/IEC 27001, realice el diseño de la etapa de planificación del SGSI, para lo cual en primera instancia se realizara un contexto de la organización, para posteriormente establecer un inventario de activos, en los cuales se podrá definir

los riesgos a los cuales se encuentran expuestos, realizar una análisis de medición de los mismos, así como la implementación de políticas que van a permitir de alguna manera el control o mitigación de estos.

1. DEFINICIÓN DEL PROBLEMA

Actualmente la EPS INDÍGENA MALLAMAS no cuenta con políticas de seguridad definidas, de igual manera no cuenta con un inventario de activos, que le permita una gestión de riesgos adecuada, lo anterior no garantiza los principios básicos de seguridad de la información y se encuentra expuesta a diferentes amenazas, las cuales han sido ya materializadas, con ataques de tipo ransomware y demás, las cuales han provocado, daños a los sistemas operativos de los servidores, perdidas de conexión a los mismos e incluso perdida de información de manera parcial, lo cual ha puesto en riesgo no solo la información, sino la continuidad del negocio, por este motivo es necesario se pueda garantizar la seguridad de la información, por ende es importante apoyarse en los marcos de referencia establecidos como la ISO/IEC 27001 y las guía de buenas prácticas de la ISO/IEC 27002, en la cual se realice el diseño de la etapa de planificación de un sistema de gestión de información.

1.1 FORMULACIÓN DEL PROBLEMA

¿Cómo el diseño de la etapa de planificación de un Sistema de gestión de seguridad de la información en el proceso de gestión de recursos físicos y tecnológicos de MALLAMAS EPS indígena puede permitir minimizar el impacto de los riesgos asociados los activos de información?

2 JUSTIFICACIÓN

La información hoy en día se ha convertido en el activo más importante para las empresas, por lo cual éste ha sido uno de los atractivos para la ciberdelincuencia, desarrollando diferentes técnicas de software malicioso, para poder vulnerarla, por este motivo al realizar la etapa de planificación de sistema de gestión de seguridad de información, permitirá reducir los riesgos de perdida de información, permitir una revisión continua de los mismos, gracias al marco normativo de la ISO/IEC 27001:2013, se podrá establecer la metodología, para la seguridad de la información, implementar medidas de seguridad para acceder a la información, así como realizar auditorías para identificar vulnerabilidades, fomentando la mejora continua.

La implementación de un SGSI demuestra a los clientes la preocupación de la entidad, frente a la confidencialidad y seguridad de la información que ha sido confiada, permite que, a cualquier situación o dificultad importante, se continúe operando con normalidad, permite el cumplimiento de la legislación vigente aplicable a la información.

En la EPS INDÍGENA MALLAMAS es necesario contar con SGSI, el cual permitirá al proceso de Gestión de recursos físicos, conocer cuáles son sus activos y administrar sus riesgos de manera adecuada, que permite ejercer controles, todo esto necesario para garantizar los pilares fundamentales del SGSI, así mismo contar con políticas de seguridad de la información, que permiten los lineamientos a cumplir por parte de la organización, para que la información cuente con la integridad, confidencialidad y disponibilidad.

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Diseñar la etapa de planificación de un sistema de gestión de seguridad en la información en el proceso de gestión de recursos físicos y tecnológicos, basados en el estándar de la norma ISO/IEC 27001:2013, para la gestión de los riesgos.

3.2 OBJETIVOS ESPECÍFICOS

- Identificar el contexto de la organización en cuanto a la seguridad de la información basado en un instrumento MSPI del ministerio de las TIC.

- Analizar los riesgos de seguridad que se encuentra asociados a cada activo de información pertenecientes al proceso gestión de recursos físicos y tecnológicos mediante la adopción de una metodología de riesgo

- Definir los controles a los riesgos de seguridad de la información con base en guía de buenas prácticas de la ISO/IEC 27002:2013

- Construir una política de seguridad de la información, a partir de buenas prácticas y referentes de seguridad que permita gestionar los riesgos a la seguridad de la información en la EPS MALLAMAS

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

4.1.1 Sistema de gestión de seguridad de la información.

Es una compilación de técnicas para realizar y controlar la privacidad de la información y la información de una entidad, de esta manera se asegura que esta información quede en manos no autorizadas.

4.1.1.1 La importancia de un SGSI.

Si bien ya se conoce aún más de acerca de la seguridad de la información, ya se empieza a conocer algún tipo de amenazas y riesgos que empiezan a determinar la importancia de la seguridad de la información, pero siempre existen algunos que no se han identificado, pero es importante conocerlas, para tomar las acciones correctivas que haya lugar.

- Robo de información. Si bien esta se puede considerar como la más obvia, pero las repercusiones van más allá, ya que esta información es fruto de muchos años de trabajo y que a veces puede superar el valor de los bienes inmuebles.

- Pérdidas económicas. Si bien la información como activo, es una pérdida económica importante, no solo es posible perderla de esta manera, en la actualidad con la transformación digital, existen diferentes métodos de transferencia electrónica, que se exponen a riesgos, los cuales muchas veces son por errores que se comenten en su uso.

- Confianza con los clientes. Las entidades deben generar confianza con sus clientes, y no permitir que sus clientes evidencies sus riesgos, por este motivo es importante que se salvaguarde la información.

- Vulnerabilidad ante la competencia. En los últimos años se ha venido exponiendo como instituciones vienen siendo atacadas con el ánimo de sabotear el trabajo, de esta manera logrando ventajas a sus competidores, igualmente no es necesario un ataque, tan solo se filtre información esta puede ser utilizadas en nuestra contra.

- Seguridad personal. Nuestra seguridad se ve expuesta cuando no cuidamos de ella, se lo ha evidenciado en el robo de información de personas de la política, empresarios, generando escándalos en redes sociales, por este motivo es importante cuidar información como de dirección de lugar de residencia, bienes, ya que esta información es insumo suficiente por los delincuentes.

- Competencia empresarial. Es necesario ver hoy en día que el tema de la seguridad es un valor importante en el mercado, esta se convierte realmente en una ventaja competitiva, ya que últimamente los clientes buscan y exigen el salvaguardar su información.

- Toma de decisiones adecuada. Cuando hablamos de tomar decisiones estas se realiza con una información la cual debe ser veraz, confidencial y completa. Las empresas pueden tomar decisiones importantes en base a esta información, la cual, si en algún momento sufra un ataque y se pierda su integridad, podría llevarnos a tomar decisiones no adecuadas que podrían llevar al declive una entidad.

4.1.2 Metodología de gestión.

En la continuidad del negocio las entidades de manera diaria deben sortear sin números de riesgos, sin embargo, la importancia de hacerle frente a estos con una buena gestión de estos es fundamental, para el alcance de sus objetivos. Cada entidad tiene la posibilidad de escoger las diferentes metodologías de administración de riesgos que existen, las cuales se describen a continuación:

ISO 31000. “Esta otra norma internacional abarca pautas para las buenas prácticas en la gestión de riesgos. Esta guía de implementación está codificada por la International Organization for Standardization. Su proceso se caracteriza por la identificación, análisis, evaluación, tratamiento, comunicación y seguimiento de cualquier tipo de riesgo que afecte a la empresa.” [3]

ISO 27005. “Norma internacional con recomendaciones y directrices generales para el Risk Management con respecto a la seguridad de la información, siguiendo los requisitos de ISO 27001. No recomienda una metodología de gestión de riesgos concreta, pero puede ser de utilidad para elaborar una propia atendiendo a diversos factores y al Sistema de Gestión de Seguridad de la Información (SGSI).”[4]

MAGERIT. “Esta metodología está desarrollada por el Consejo Superior de Administración Electrónica en España. Consta de los volúmenes de método, catálogo de elementos para aplicar la metodología y guía de técnicas a usar en las diferentes fases del Risk Management.” [5]

---

[3] EALDE Business School. Metodologías en Gestión de Riesgos. [Sitio web]. [Consulta: 25 de Marzo de 2021]. “Disponible en: https://www.ealde.es/metodologias-gestion-riesgos/”

[4] Ibid., p1

[5] Ibid., p2

OCTAVE. “Esta metodología reconocida internacionalmente está desarrollada por el Software Engineering Institute. Octave proporciona un conjunto de criterios a partir de los cuales se pueden desarrollar distintas metodologías. Está compuesta de las fases de visión de organización, visión tecnológica y planificación de medidas y reducción de los riesgos.” [6]

NIST 800-30. “Esta metodología desarrollada por el National Institute of Standards and Technology tiene reconocimiento internacional y busca asegurar a los sistemas de información. Sus pasos básicos para la gestión de riesgos son la caracterización del sistema, identificación de amenazas y vulnerabilidades, control de análisis, determinación del riesgo, análisis de impacto, determinación del riesgo, recomendaciones de control y resultado de la implementación o documentación.” [7]

CRAMM. “Tiene reconocimiento internacional y está desarrollada por el Central Computer and Telecommunications Agency (CCTA). Su desarrollo consta de identificación y valoración de activos, valoración de amenazas y vulnerabilidades y selección de contramedidas.

Las empresas han de considerar estas metodologías en gestión de riesgos y escoger e implementar aquellas que se ajusten más a su naturaleza y al sector en el que desempeñan su actividad.”[8]

---

[6] EALDE Business School. Metodologías en Gestión de Riesgos. [Sitio web]. [Consulta: 25 de Marzo de 2021]. “Disponible en: https://www.ealde.es/metodologias-gestion-riesgos/”

[7] Ibid., p4

[8] Ibid., p5

4.1.3 **El modelo de seguridad y privacidad de la información – MSPI.**

Proporciona los lineamientos para implementar y adoptar las buenas prácticas, de acuerdo con los estándares internacionales, el objetivo es que las entidades de carácter público “incorporen la seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y, en general, en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.”[9]

El MSPI “Sé encuentra alineado con el Marco de Referencia de Arquitectura TI, el Modelo Integrado de Planeación y Gestión (MIPG) y La Guía para la Administración del Riesgo y el Diseño Controles en entidades Públicas, este modelo pertenece al habilitador transversal de Seguridad y Privacidad, de la Política de Gobierno Digital. Y Se desarrolla mediante el Documento Maestro del Modelo de Seguridad y Privacidad de la Información y sus guías de orientación. Lo debe desarrollar el líder o encargado de Seguridad de la Información con el apoyo de toda la estructura organizacional.”[10]

4.2 MARCO CONCEPTUAL

SGSI. “Un sistema de gestión de la seguridad de la información es, como el nombre lo sugiere, un conjunto de políticas de administración de la información. El término es utilizado principalmente por la ISO/IEC 27001, aunque no es la única normativa

---

[9] MSPI. “Modelo de Seguridad y Privacidad de la Información. [Sitio web]. [Consulta: 26 de Marzo de 2021]. Disponible en: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/”

[10] MSPI. “Modelo de Seguridad y Privacidad de la Información. [Sitio web]. [Consulta: 26 de Marzo de 2021]. Disponible en: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/

que utiliza este término o concepto. Un SGSI es para una organización el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información."[11]

INFORMACIÓN. "La información es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje." [12]

SEGURIDAD DE LA INFORMACIÓN: "La información es un recurso que, como el resto de los activos, tiene valor para una organización y por consiguiente debe ser debidamente protegida. La seguridad de la información protege ésta de una amplia gama de amenazas, a fin de garantizar la continuidad del negocio, minimizar el daño al mismo y maximizar el retorno sobre las inversiones y las oportunidades."[13]

---

[11] Colaboradores de Wikipedia. "Sistema de gestión de la seguridad de la información. [Sitio web]. [Consulta: 25 de Marzo de 2021]. Disponible en: https://es.wikipedia.org/wiki/Sistema_de_gesti%C3%B3n_de_la_seguridad_de_la_informaci%C3%B3n"

[12] Colaboradores de Wikipedia. (2021c, marzo 2). Información. Wikipedia, la enciclopedia libre. . [Sitio web]. [Consulta: 25 de Marzo de 2021]. Disponible en: https://es.wikipedia.org/wiki/Informaci%C3%B3n#:%7E:text=Informaci%C3%B3n%20es%20el%20nombre%20por,sistema%20que%20recibe%20dicho%20mensaje.&text=En%20biolog%C3%ADa%2C%20la%20informaci%C3%B3n%20se,al%20comportamiento%20de%20los%20individuos

[13] colaboradores de Wikipedia. Seguridad de la información. Wikipedia, la enciclopedia libre. [Consulta: 25 de Marzo de 2021]. Disponible en: https://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n

CONFIDENCIALIDAD. “Asegurar que solo quienes estén autorizados pueden acceder a la información.”[14]

INTEGRIDAD. “Asegurar que la información y sus métodos de proceso son exactos y completos.” [15]

DISPONIBILIDAD. Asegurar que los usuarios autorizados tengan acceso a la información y a sus activos asociados cuando lo requieran.

4.3 MARCO CONTEXTUAL

4.3.1 Reseña histórica de la EPS MALLAMAS.

MALLAMAS EPS INDÍGENA, “Es una entidad de carácter especial, sin ánimo de lucro, autorizada y vigilada por la Superintendencia Nacional de Salud comprometida con la salud, progreso y desarrollo de la comunidad en Nariño y todo el País.

MALLAMAS EPS INDÍGENA, nace por iniciativa y gestión de líderes indígenas de la comunidad de los Pastos, en el Resguardo Indígena de Muellamues Municipio de Guachucal (Nariño), en el año de 1995, inicialmente se construyó como empresa solidaria de salud que presta sus servicios a sus asociados, hacia el año 1996 por Resolución emanada por la Superintendencia Nacional de Salud, es autorizada para administrar los recursos del Régimen Subsidiado.

---

[14] Firma-e. Pilares de la Seguridad de la Información: confidencialidad, integridad y disponibilidad [Sitio web]. [Consulta: 26 de Marzo de 2021]. Disponible en: https://www.firma-e.com/blog/pilares-de-la-seguridad-de-la-informacion-confidencialidad-integridad-y-disponibilidad/

[15] Ibid., p1

La empresa inicia su gestión con 5000 afiliados, a finales de 1996 cuenta con 28.000 gracias a la consolidación patrimonial la Supersalud mediante resolución 0338 de 28 de abril de 1997 amplia a 130.000 beneficiarios la capacidad de afiliación de la empresa y su cobertura geográfica a 32 municipios.

En él años 1998 y por evaluación realizada por el ministerio de salud a través de CINDER y la universidad de Valle, es calificada como la mejor empresa solidaria de salud de Nariño y una de las 10 primeras del País

En 1999 se realiza el convenio ETNOSALUD conformado por la ESS GUAITARA, la cooperativa Alcatraz y la ESS MALLAMAS, el cual termina por exigencias gubernamentales expresadas a través del decreto 1804 del mismo año.

En el año 2000 por las exigencias normativas del Gobierno Nacional, entra en proceso de incorporación; sin embargo y debido a las consideraciones y lucha de las Administradoras del Régimen Subsidiado creadas y conformadas por las Autoridades Indígenas, se logra consolidar el proceso de trasformación en EPS INDÍGENA.

En el año 2.006 la Superintendencia Nacional de Salud emite la resolución No. 00332 *Por medio de la cual se resuelve sobre la solicitud de habilitación de la entidad MALLAMAS EPS-I* para administrar y operar el Régimen Subsidiado del Sistema General de Seguridad Social en Salud. Posteriormente, mediante la Resolución 301 del 17 de marzo de 2008, la Superintendencia Nacional de Salud autoriza la habilitación de MALLAMAS EPS I para administrar el régimen subsidiado. Actualmente la EPS INDÍGENA MALLAMAS se fortalece como una de las entidades más sólidas del Departamento y del País."[16]

[16] MALLAMAS EPS INDÍGENA, Reseña Histórica, [Sitio Web] Ipiales – Nariño [Consultado el 28 de Marzo de 2021] Disponible en: https://www.mallamaseps.com.co/index.php/component/k2/item/3-

4.3.2 Misión.

“Somos una entidad pública de carácter especial con enfoque diferencial indígena, que trabaja por el derecho fundamental de la salud, a través del aseguramiento y gestión del riesgo, para contribuir con el buen vivir de la población afiliada, con calidad, sentido humano, respetando la diversidad étnica y cultural.”

4.3.3 Visión.

“En el año 2020 seremos una organización indígena altamente competitiva, líder en el aseguramiento y la gestión del riesgo en salud, con talento humano comprometido en el mejoramiento continuo de los procesos, la satisfacción de los usuarios, respetando y promoviendo la diversidad etno-cultural de nuestra población afiliada”[17]

4.3.4 Mapa de procesos.

La entidad cuenta con cuatro macroprocesos los cuales son Macroproceso de Dirección, Misionales, De control y Apoyo, los cuales los conforma diferentes procesos como se evidencias en la figura 1.

---

resena-historica#:~:text=MALLAMAS%20EPS%20INDIGENA%2C%20nace%20por,hacia%20el%20a%C3%B1o%201996%20por

[17] MALLAMAS EPS INDÍGENA, Plataforma estratégica, [Sitio Web] Ipiales – Nariño [Consultado el 28 de Marzo de 2021] Disponible en: https://www.mallamaseps.com.co/index.php/nosotros/plataforma

Figura 1 Mapa de Procesos MALLAMAS EPS INDÍGENA

Fuente. Plataforma estratégica MALLAMAS EPS Indígena

4.3.5 Procedimientos del proceso de Gestión de Recursos Físicos y tecnológicos.

Dentro del proceso de gestión de recursos físicos y tecnológicos, en el presente proyecto nos centraremos en dos procedimientos los cuales corresponden al procedimiento de Mantenimiento Preventivo y Correctivo de Equipos de Cómputo y Comunicaciones, como al procedimiento de gestión de backups.

4.4 MARCO LEGAL

“Circular 052 de 25 de octubre de 2007, de la Superintendencia Financiera de Colombia. Requerimientos mínimos de seguridad y calidad en el manejo de

información a través de medios y canales de distribución de productos y servicios para clientes y usuarios."[18]

"Ley 1266 de 31 de diciembre de 2008, por la cual se dictan las disposiciones generales del habeas 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."[19]

"Resolución 2258 de 21 de diciembre de 2009 CRC, de la Comisión de Regulación de las Comunicaciones, por la cual se modifican los artículos 22 y 23 de la Resolución 1732 de la CRT de 2007 y los artículos 1,8 y 2,4 de la Resolución 1740 de la CRT de 2007."[20]

"Ley 1273 del 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"[21]

---

[18] SUPERINTENDENCIA FINANCIERA, Normatividad Circular 052 de Octubre de 2007 [Sitio Web] [Consultado el 28 de Marzo de 2021] Disponible en : https://www.superfinanciera.gov.co/jsp/Publicaciones/publicaciones/loadContenidoPublicacion/id/20072/dPrint/1/c/00

[19] Ley 1266 de 208, Secretaria del Hábitat. [Sitio Web] [Consultado el 28 de Marzo de 2021] Disponible en : https://www.habitatbogota.gov.co/transparencia/normatividad/normatividad/ley-1266-2008#:~:text=Descripci%C3%B3n%3A,y%20se%20dictan%20otras%20disposiciones.

[20] Normograma CRC [RESOLUCION_CRC_2258_2009]. [Sitio Web] [Consultado el 28 de Marzo de 2021] Disponible en : https://normograma.info/crc/docs/resolucion_crc_2258_2009.htm

[21] Ley 1273 de 2009, Secretaria del Hábitat. [Sitio Web] [Consultado el 28 de Marzo de 2021] Disponible en : https://www.habitatbogota.gov.co/transparencia/marco-legal/normatividad/ley-1273-2009#:%7E:text=Descripci%C3%B3n%3A,las%20comunicaciones%2C%20entre%20otras%20disposiciones.

ISO. “Originalmente en inglés: International Organization for Standardization, conocida por las siglas ISO, es una organización para la creación de estándares internacionales compuesta por diversas organizaciones nacionales de estandarización. Fundada el 23 de febrero de 1947, la organización promueve el uso de estándares propietarios, industriales y comerciales a nivel mundial. Su sede está en Ginebra (Suiza) y hasta 2015 trabajaba en 196 países.”[22]

ICONTEC. “El Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC, es el organismo nacional de normalización, según el Decreto 2269 de 1993. ICONTEC es una entidad de carácter privado, sin ánimo de lucro, cuya Misión es fundamental para brindar soporte y desarrollo al productor y protección al consumidor. Colabora con el sector gubernamental y apoya al sector privado del país, para lograr ventajas competitivas en los mercados interno y externo.”[23]

ISO 27001. “ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.”[24]

---

[22] Colaboradores de Wikipedia. Organización Internacional de Normalización. Wikipedia, la enciclopedia libre. [Sitio web]. [Consulta: 26 de Marzo de 2021]. Disponible en: https://es.wikipedia.org/wiki/Organizaci%C3%B3n_Internacional_de_Normalizaci%C3%B3n”

[23] Icontec. Quiénes somos. [Sitio web]. [Consulta: 26 de Marzo de 2021]. Disponible en: https://www.icontec.org/quienes-somos/

[24] 27001Academy. ¿Qué es norma ISO 27001? [Sitio web]. [Consulta: 26 de Marzo de 2021]. Disponible en: https://advisera.com/27001academy/es/que-es-iso-

ISO/IEC 27002: “es una guía que contiene las buenas prácticas para llevar a cabo la implementación de un SGSI, de acuerdo con los lineamientos de la ISO/IEC 27001.”[25]

27001/#:%7E:text=ISO%2027001%20es%20una%20norma,ISO%2FIEC%2027001%3A201327001/#:~:text=ISO%2027001%20es%20una%20norma,ISO%2FIEC%2027001%3A2013.

[25] ISO 27002: Buenas prácticas para gestión de la seguridad de la información. OSTEC | Segurança digital de resultados. [Sitio web]. [Consulta: 26 de Marzo de 2021]. Disponible en: https://ostec.blog/es/generico/iso-27002-buenas-practicas-gsi/

5 DISEÑO METODOLÓGICO

La metodología descriptiva será la utilizada para llevar a cabo la etapa de planificación de un sistema de gestión de seguridad en la información que permita al área de las TIC, basados en el estándar de la norma ISO/IEC 27001:2013 , teniendo en cuenta que es necesario conocer el contexto actual de la organización, permitiendo la descripción de esto de forma sistémica, en donde gracias a esta metodología vamos a realizar un análisis, a través de la recolección de información, que permitirá describir e interpretar todo lo anterior basado en el marco de trabajo de la ISO/IEC27001/:2013, así como adoptar la guía de buenas prácticas establecidas en la ISO/IEC 27002:2013

5.1 TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN

Para este proyecto aplicado se realizará las siguientes técnicas de recolección de información.

Cuadro 1. Instrumentos de recolección de información

TÉCNICA	DESCRIPCIÓN
Observación	Técnica que se utiliza para estudiar la muestra en donde se tiene un enfoque claro del estado actual de la entidad
Revisión de documentos	Esta técnica nos permite revisar el estado actual de la entidad y realizar una proyección de esta

Cuadro 1 (Continuación)

TÉCNICA	DESCRIPCIÓN
Entrevista	En esta, para obtener información se realiza preguntas de forma personal de manera directa y verbal
Encuesta	Se realiza mediante encuestas estructuradas con preguntas abiertas y cerradas

Fuente. Propia

5.2 POBLACIÓN

La población está compuesta por los integrantes de la coordinación de informática de la EPS INDÍGENA MALLAMAS

5.3 MUESTRA

Se define como la población a cuatro funcionarios de la empresa MALLAMAS EPS INDÍGENA de la coordinación de informática.

6 DIAGNOSTICO DE SEGURIDAD DE LA INFORMACIÓN

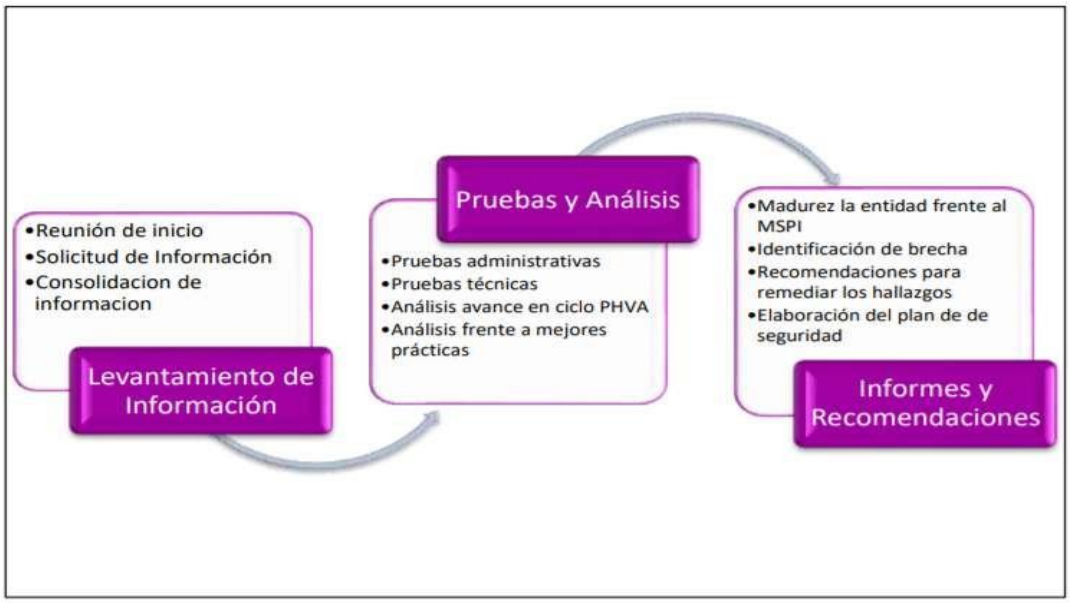
La seguridad de la información se define como aquel conjunto de medidas y técnicas empleadas para controlar y salvaguardar todos los datos que se manejan dentro de una empresa o institución y de esta manera asegurar que estos no salgan del sistema establecido por la empresa.

También se considera, una pieza clave para que estas empresas puedan llevar a cabo sus operaciones, ya que los datos manejados son esenciales para la actividad que desarrollan, el diagnostico de seguridad de información nos brindara la pauta para poder saber como se encuentra actualmente la empresa.

6.1 CONTEXTO DE LA ENTIDAD

Mediante el modelo de seguridad y privacidad de información, desarrollada por el ministerio de las TIC, se desarrollará la herramienta de diagnóstico de seguridad y privacidad de la información. Para lo cual y como se refleja en la Figura 2, se realizara unas fases que nos permitirán realizar este autodiagnóstico, la cual se comienza realizando el levantamiento de la información, en donde se comprende una reunión inicial, en la cual se solicitara la información para ser consolidada, Posteriormente se realiza el diligenciamiento en esta herramienta, frente a las pruebas de tipo administrativas, técnicas, etc... lo que al final con la información recolectada, se obtendrá un informe frente al madurez frente MSPI, identificación de la brecha, para dar paso a la elaboración o planificación del SGSI.

Figura 2 Desarrollo de la Metodología de Autodiagnóstico



Fuente. Instructivo para el Diligenciamiento de la Herramienta de Diagnostico

6.1.1 Levantamiento de la Información.

Se realizo la aplicación de la herramienta de diagnóstico de seguridad y privacidad de la información, la cual fue desarrollada, teniendo en cuenta el instructivo para el diligenciamiento de esta construido por el mismo ministerio de las TIC's, de acuerdo con las reuniones realizadas con el personal de la entidad en donde se verifico la existencia de la información y la indagación de los ítems propuestos, se pudo determinar en la tabla 1, el siguiente diagnóstico.

Tabla 1 Evaluación de efectividad de controles.

No.	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	0	60	**INEXISTENTE**
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	9	30	**INICIAL**
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	26	57	**REPETIBLE**
A.8	GESTIÓN DE ACTIVOS	6	46	**INICIAL**
A.9	CONTROL DE ACCESO	5	57	**INICIAL**
A.10	CRIPTOGRAFÍA	0	0	**INEXISTENTE**
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	11	59	**INICIAL**
A.12	SEGURIDAD DE LAS OPERACIONES	9	54	**INICIAL**
A.13	SEGURIDAD DE LAS COMUNICACIONES	14	67	**INICIAL**
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	3	48	**INICIAL**
A.15	RELACIONES CON LOS PROVEEDORES	0	50	**INEXISTENTE**
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	0	60	**INEXISTENTE**
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	4	43,5	**INICIAL**
A.18	CUMPLIMIENTO	7,5	60	**INICIAL**
	PROMEDIO EVALUACIÓN DE CONTROLES	**7**	**49**	**INICIAL**

Fuente. Propia

En la Figura 3, es posible determinar el espacio o brecha en el cual se encuentra, la EPS en el cumplimiento de lo establecido en el anexo A de la norma ISO 27001:2013,

Figura 3 Brecha de Anexo a ISO 27001:2013

Fuente. Propia

De acuerdo con la información arrojada, esta es consecuente ya que demuestra la no existencia de un sistema de gestión de seguridad de la información y que algunas de las medidas que se han tomado son productos de situaciones empíricas o por la experiencia de hechos que han ocurrido, por cuanto teniendo en cuentas esta situación se plantea un objetivo de cumplimiento con el desarrollo de este proyecto en un 40%, ya que en la fase de implementación, es donde se encuentra la mayor complejidad en el desarrollos del sistema de gestión de información

De esta manera es claro que la entidad, al no tener implementado un sistema de gestión de información, por cuanto igualmente carece de avances en el ciclo de funcionamiento del modelo de operaciones PHVA, el cual de acuerdo autodiagnóstico arrojo la información en la Tabla 2.

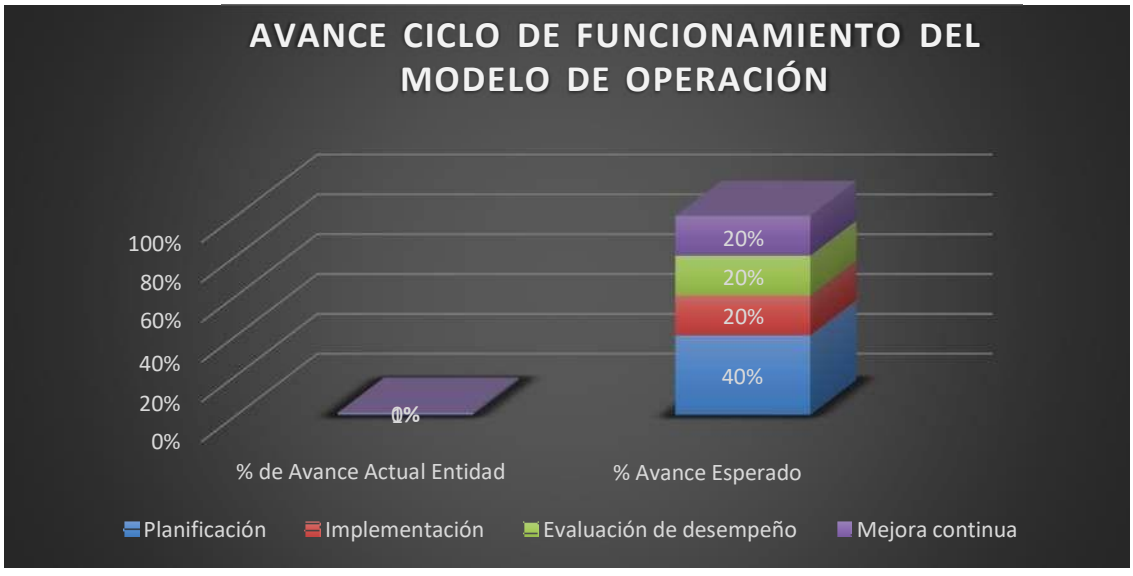
Tabla 2. Avance PHVA

Año	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2021	Planificación	1%	40%
	Implementación	0%	20%
	Evaluación de desempeño	0%	20%
	Mejora continua	0%	20%
	TOTAL	**1%**	**100%**

Fuente. Propia

En Figura 3 se pude evidenciar de manera gráfica, el avance que se espera por cada fase una vez se implemente el SGSI, igualmente al no tener implementación del SGSI, los datos arrojados son mínimos.

Figura 3 Grafica avance PHVA.



Fuente. Propia

En la herramienta es posible determinar el nivel de madurez del modelo de seguridad y privacidad de la información en donde se determinarlos rangos

establecidos, de acuerdo con el porcentaje obtenido, como se evidencia en la siguiente tabla 3:

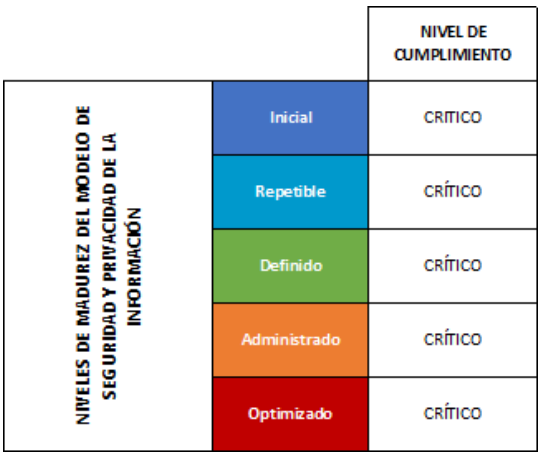
Tabla 3. Rangos de calificación

TOTAL DE REQUISITOS CON CALIFICACIONES DE CUMPLIMIENTO	
CRÍTICO	0% a 35%
INTERMEDIO	36% a 70%
SUFICIENTE	71% a 100%

Fuente. Herramienta MSPI

Para poder determinar el nivel de cumplimiento de madurez, la herramienta, establece varios parámetros empezando por una madurez denominada “inicial” y la última como “optimizado”, en donde es posible calificar el nivel, de acuerdo con la gráfica anteriormente explicada.

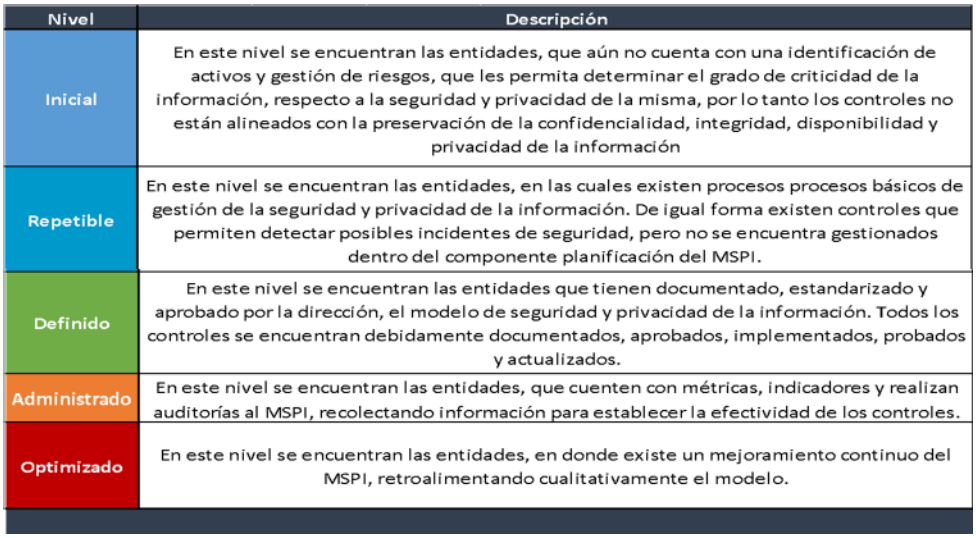
Figura 5. Nivel de Cumplimiento de madurez.



Fuente. Fuente Propia

Para una mejor comprensión en la Figura 6, es posible determinar y describir a que hace referencia cada uno de los diferentes niveles de madurez del modelo.

Figura 6 Descripción de Niveles de Madurez



Nivel	Descripción
Inicial	En este nivel se encuentran las entidades, que aún no cuenta con una identificación de activos y gestión de riesgos, que les permita determinar el grado de criticidad de la información, respecto a la seguridad y privacidad de la misma, por lo tanto los controles no están alineados con la preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información
Repetible	En este nivel se encuentran las entidades, en las cuales existen procesos procesos básicos de gestión de la seguridad y privacidad de la información. De igual forma existen controles que permiten detectar posibles incidentes de seguridad, pero no se encuentra gestionados dentro del componente planificación del MSPI.
Definido	En este nivel se encuentran las entidades que tienen documentado, estandarizado y aprobado por la dirección, el modelo de seguridad y privacidad de la información. Todos los controles se encuentran debidamente documentados, aprobados, implementados, probados y actualizados.
Administrado	En este nivel se encuentran las entidades, que cuenten con métricas, indicadores y realizan auditorías al MSPI, recolectando información para establecer la efectividad de los controles.
Optimizado	En este nivel se encuentran las entidades, en donde existe un mejoramiento continuo del MSPI, retroalimentando cualitativamente el modelo.

Fuente. Herramienta de diagnóstico MSPI

Igualmente, la herramienta de diagnóstico determina la calificación frente a las mejores prácticas en ciberseguridad (NIST), en donde de acuerdo con los valores arrojados se obtuvo una calificación, la cual se discrimina de acuerdo con cada uno de sus componentes:

Identificar. Se califica la gestión de activos, el ambiente de negocio, la evaluación del riesgo y la estrategia de gestión de riesgos.

Proteger. Se califica el control de acceso, capacitación y sensibilidad, Seguridad de datos, Protección de información y procedimiento, Mantenimiento y tecnología de protección.

Detectar. Se califica Anomalías y eventos, Monitoreo continuo de la seguridad y proceso de detección.

Responder. Se califica planes de respuesta, Comunicaciones, Análisis, mitigación y mejoras.

Recuperarse. Se califica planes de recuperación, Mejoras y comunicaciones.

En donde al final arrojo los siguientes resultados:

Tabla 4 Calificación de componentes NIST

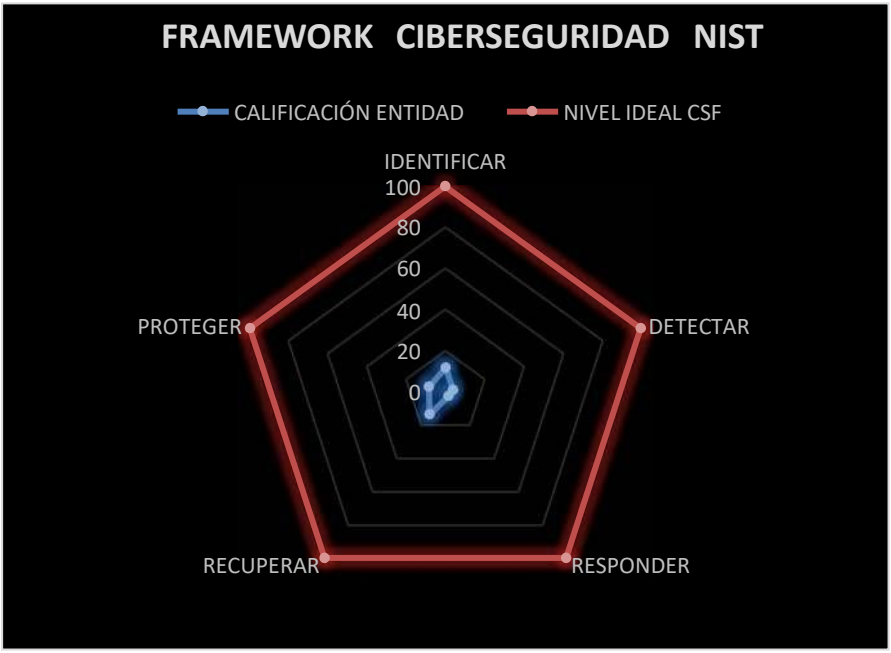
MODELO FRAMEWORK CIBERSEGURIDAD NIST

Etiquetas de fila	CALIFICACIÓN ENTIDAD	NIVEL IDEAL CSF
IDENTIFICAR	12	100
DETECTAR	4	100
RESPONDER	2	100
RECUPERAR	13	100
PROTEGER	9	100

Fuente. Propia.

Para una mayor comprensión en la figura 7, es posible observar el cumplimiento y la brecha de acuerdo del nivel de calificación correspondiente al marco de las NIST,

Figura 7. Grafica Nivel de Calificación de la entidad CSF



Fuente. Propia

De acuerdo con los valores arrojados en cada uno de los ítems antes expuestos de acuerdo con la herramienta, estos ratifican la no existencia de un sistema de seguridad de la información, por lo anterior para realizar un diseño de sistema de seguridad de la información es necesario, realizar un inventario de activos que nos permita identificar los riesgos de estos, para lo cual es necesario adoptar metodologías que permitan una buena gestión de los mismo.

7 INVENTARIO DE ACTIVOS

El inventario y clasificación de los Activos de Información es la base para la gestión de riesgos de seguridad de la información y para determinar los niveles de protección requeridos.

Se denomina activo a aquello que tiene algún valor, por tanto, debe protegerse. De manera que un Activo de Información incluye la información estructurada y no estructurada que se encuentre presente en forma impresa, escrita en papel, transmitida por cualquier medio electrónico o almacenada en equipos de cómputo, incluyendo datos contenidos en registros, archivos y bases de datos. Así mismo, un Activo de Información tiene el mismo valor, bien sea que se encuentre forma física o digital, aunque los controles necesarios para protegerlo son diferentes.

Para realizar el inventario de activos se realizará mediante la metodología MAGERIT V 3.0, la cual clasifica en ocho grupos los cuales se clasificarán más adelante.

7.1.1 Activos.

Es necesario identificar los activos de con que cuenta MALLAMAS EPS INDÍGENA, según Magerit v3, teniendo en cuenta que un activo "es un componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos" [26]. Si se quiere la

[26] Pilar. "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método. Magerit 3.0. Madrid. Subdirección General de Información, Documentación y Publicaciones. 2012. P. 22 Disponible en: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html"

realización de un correcto inventario de activos de MALLAMAS EPS INDÍGENA es necesario la identificación de cada uno de los componentes que son primordiales para la entidad, que sin estos no se realizara llevar a cabo su objetivo.

7.1.2 Proceso de estudio.

Este corresponde al proceso de Gestión de Recursos Físicos y Tecnológicos

Cuadro 2. Procesos Gestión de Recursos Tecnológicos

Proceso	Descripción
GESTIÓN DE RECURSOS FÍSICOS Y TECNOLÓGICOS	En el proceso se realiza el procedimiento de mantenimiento preventivo, correctivo de los elementos de cómputo de la entidad como su solicitud de adquisición

Fuente: Procesos MALLAMAS EPS Indígena

Teniendo en cuenta la metodología MAGERIT, necesario realizar la definición de los diferentes tipos de activos.

7.1.2.1 Tipos de activos.

A continuación, se mencionan los tipos de activos de acuerda a la metodología

- **[d] datos/información**. Este se refiere a todos los datos que son procesados, que crean, almacenan y que logran que la entidad cumpla con sus procesos.

- **[s] servicios.** Se refiere a aquellos servicios que se brindan con éxito, para que funcione los procesos de la entidad. Su funcionabilidad satisface las necesidades del usuario interno o externo.

- **[sw] software - aplicaciones informáticas.** Se refiere a todos estos aplicativos que procesan los datos para llevar a cabo el cumplimiento de los procesos de MALLAMAS Eps

- **[hw] hardware - equipos informáticos.** Se refiere a todo el hardware que se encuentran los aplicativos informáticos, al igual que datos, servicios y que se utilizan para los procesos.

- **[com] redes de comunicaciones.** Se refiere a los elementos que su función es el intercambio de datos o permiten conectar la red, entre estos los routers, swicht, Etc…

- **los soportes de información.** Se refiere a esos dispositivos físicos que nos sirven para el almacenamiento de manera permanente o parcial, como discos duros, cintas magnéticas etc...

- **el equipamiento auxiliar.** Se refiere a dispositivos que su función es el soporte a los sistemas de información, sin estar directamente relacionados con datos.
- **las instalaciones.** Se refiere a los lugares en donde se encuentran los dispositivos informáticos y de comunicación.

- **las personas.** Se refiere a las personas que utilizan o se relacionan con los activos nombrados anteriormente.

7.1.3 Inventario de Activos de MALLAMAS EPS INDÍGENA.

En el Cuadro 3, es posible determinar de acuerdo con la clasificación década activo, su nombre y una breve descripción, que permitirá comprender de manera más adecuada, lo que cuenta la entidad para el desarrollo de este proceso.

Cuadro 3. Inventario Activos.

Tipo	Nombre	Descripción
INFORMACIÓN/DATOS.	Bd de inventario de equipos.	Bd en las cuales se registra la asignación de los equipos de computo
	Bd. de solicitudes soportes técnicos	Bd en las cuales se registra las Solicitudes de los funcionarios con respecto a soportes técnicos
	Copias de seguridad.	Dispositivo donde se almacena copias de seguridad.
	Documentos colaboradores	Archivos locales de los colaboradores.
APLICACIONES INFORMÁTICAS.	Aplicación web.	Aplicación de gestión de inventario de equipos
	Aplicaciones Comerciales.	Sistemas operativos, Office, Antivirus.
	Aplicación osticket	Se encarga de administrar las solicitudes de soporte técnico.
	Cliente de correo electrónico.	Se encarga de la recepción de los correos corporativos

Cuadro 3 (Continuación)

Tipo	Nombre	Descripción
EQUIPOS INFORMÁTICOS.	(4) Computadores Colaboradores.	Estaciones de trabajo de colaboradores de coordinación de informática
	Servidores	Equipo donde se centra la información y aplicativos para operar las actividades del área
REDES DE COMUNICACIONES.	Router.	conexión canal dedicado con router
	Conexión Internet	Permite la interconexión de datos entre sucursales. Y brinda acceso a aplicativos webs.
	Red local.	LAN de MALLAMAS EPS INDÍGENA
SERVICIOS.	Servicio de conectividad.	Servicio en donde se accede a la intranet de empresa.
	Sistema de correo electrónico.	Servicio de correo electrónico contratado
	Soporte TIC	Es el servicio que brinda soporte a los sistemas de información
PERSONAL.	Colaboradores.	Colaboradores MALLAMAS EPS INDÍGENA
	Proveedor tecnológico	
SOPORTES DE INFORMACIÓN	Discos duros	Backups del servidor
INSTALACIONES.	Oficina	Oficinas coordinación de informática

Fuente: Propia

7.1.3.1 Dimensionar la Valoración.

En esta se valora de manera cuantitativa cada dimensión:

“Disponibilidad, Integridad de los datos, Confidencialidad de los datos”

7.1.3.2 Criterios de Valoración Cuantitativa

Es necesario para realizar una valoración de tipo cuantitativa usar un rango común que permite la comparación de riesgos, como se puede mostrar en la figura 8.

Figura 8. Escala de valor de activos Cualitativa.

VALORACIÓN DEL RIESGO			
	Nomenclatura	Categoría	Valoración
Valoracion del riesgo	MA	Critico	21 a 25
	A	Importante	16 a 20
	M	Apreciable	10 a 15
	B	Bajo	5 a 9
	MB	Despreciable	1 a 4

Fuente: Metodología Magerit.

De acuerdo con las escalas de valores de activos definidos en la anterior figura, se realizó en el cuadro 3. en conde se realiza la clasificación de las tres dimensiones, en lo que comprende la confidencialidad, integridad y disponibilidad de la información.

Cuadro 4 Valoración del Activo Cuantitativo

No.	Nombre del activo de información	Tipo de Activo	Dimensiones		
			Confidencialidad	Integridad	Disponibilidad
1	Base de datos de inventario de Equipos	DATOS	M	MA	MA
2	Base de datos de solicitudes de soportes técnicos	DATOS	B	M	MA
3	Copias de Seguridad	DATOS	MA	MA	MA
4	Documentos de personal	DATOS	M	B	M
5	Aplicaciones web osticket	SOFTWARE	B	B	MA
6	Aplicación web inventario de equipos	SOFTWARE	M	MA	MA
7	Aplicaciones de ofimática	SOFTWARE	M	B	MA
8	Cliente de correo electrónico	SOFTWARE	M	M	MA
9	Computadores de funcionarios	HARDWARE	M	M	M
10	Servidores	HARDWARE	MA	MA	MA
11	Routers	HARDWARE	MA	MA	MA
12	Conexión a internet	COMUNICACIONES	MA	MA	MA
13	Red local	COMUNICACIONES	MA	MA	MA
14	Servicios de conectividad	SERVICIOS	MA	MA	MA
15	sistema de correo electrónico	SERVICIOS	MA	MA	MA
16	soporte Tic	PERSONAL	B	MA	MA
17	Colaboradores	PERSONAL	M	M	M
18	Proveedor Tecnológico	PERSONAL	M	M	M
19	Discos Duros	SOPORTE	MA	MA	MA
20	Oficina	INSTALACIONES	M	M	MA

Fuente: Metodología Magerit.

7.1.3.3 Criterios de Valoración Cuantitativos

El valor del activo es el resultado de realizar el promedio de las tres (3) dimensiones D,I,C y su correspondiente clasificación se realiza de acuerdo con la Figura 4 siguiente:

Figura 4: Escala valor activo Cuantitativa.

VALORACIÓN DEL RIESGO			
	Nomenclatura	Categoría	Valoración
Valoracion del riesgo	MA	Critico	21 a 25
	A	Importante	16 a 20
	M	Apreciable	10 a 15
	B	Bajo	5 a 9
	MB	Despreciable	1 a 4

Fuente. Magerit

Al igual como se realizó la valoración de los activos de manera cualitativa, estos se realizan de manera cuantitativa de acuerdo con la anterior escala, en donde se contempla igualmente las tres (3), dimensiones, con la diferencia que se realiza el promedio de los tres valores, como se evidencia en la anterior grafica.

Cuadro 5 Valoración de activos.

	Nombre	Riesgo	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR
1	Base de datos de inventario de Equipos	CRITICO	15	25	25	22
2	Base de datos de solicitudes de soportes técnicos	IMPORTANTE	9	15	25	16
3	Copias de Seguridad	CRITICO	25	25	25	25
4	Documentos de personal	APRECIABLE	15	9	15	13
5	Aplicaciones web osticket	APRECIABLE	9	9	25	14
6	Aplicación web inventario de equipos	CRITICO	15	25	25	22
7	Aplicaciones de ofimática	IMPORTANTE	15	9	25	16
8	Cliente de correo electrónico	IMPORTANTE	15	15	25	18
9	Computadores de funcionarios	APRECIABLE	15	15	15	15
10	Servidores	CRITICO	25	25	25	25
11	Routers	CRITICO	25	25	25	25
12	Conexión a internet	CRITICO	25	25	25	25
13	Red local	CRITICO	25	25	25	25
14	Servicios de conectividad	CRITICO	25	25	25	25
15	sistema de correo electrónico	CRITICO	25	25	25	25
16	soporte Tic	IMPORTANTE	9	25	25	20
17	Colaboradores	APRECIABLE	15	15	15	15
18	Proveedor Tecnológico	APRECIABLE	15	15	15	15
19	Discos Duros	CRITICO	25	25	25	25
20	Oficina	IMPORTANTE	15	15	25	18

Fuente: Metodología Magerit.

En la tabla 7 se realiza la contabilización de cada uno de los activos, pero de acuerdo con su tipo de activo, en el marco de la metodología MAGERIT.

Tabla 7 Clasificación según el Tipos de Activos

Tipo de activo	Cantidad
Tipo Dato	4
Tipo Claves Criptográficas	0
Tipo Servicio	2
Tipo Software	4
Tipo Hardware	3
Tipo Comunicaciones	2
Tipo Soporte de Información	1
Tipo Equipamiento Auxiliar	0
Tipo Instalaciones	1
Tipo Personal	3
Total de Activos	20

Fuente. Propia

En la tabla 8 se realiza la contabilidad de los activos, de acuerdo con el impacto.

Tabla 8 Clasificación según el impacto

Clasificación según impacto a la seguridad	
Leve	4
Importante	10
Grave	6

Fuente. Propia

Igualmente se realiza la contabilidad de los activos por su nivel de riesgo, en lo cual se establece las escalas desde la baja hasta el extremo.

Tabla 9 Clasificación según el nivel del riesgo

Resumen de nivel de riesgo en los activos	
Extremo	10
Alto	5
Medio	4
Bajo	1

Fuete. Propia

En la figura 9 es posible identificar la clasificación de los activos de acuerdo con el nivel de riesgo, en donde es posible determinar que el extremo es más representativo.

Figura 9 Clasificación según el nivel del riesgo

Fuente. Propia

En la tabla 10 es posible determinar los activos de acuerdo con su ubicación si se trata de Física o Electrónica,

Tabla 10 Clasificación según su ubicación

Ubicación	
Física	7
Electrónica	13

Fuente. Propia

En el Cuadro 5 se realiza la valoración de los activos de acuerdo con la escala de criterios comunes (C.C.), y se califican por las tres dimensiones.

Cuadro 6 Valoración de los activos en escala C.C.

Nombre	Riesgo	Confidencialidad	Integridad	Disponibilidad	Valor
Base de datos de inventario de Equipos	EXTREMO	5	9	9	8
Base de datos de solicitudes de soportes técnicos	ALTO	3	5	9	6
Copias de Seguridad	EXTREMO	9	9	9	9
Documentos de personal	BAJO	5	3	5	4
Aplicaciones web osticket	MEDIO	3	3	9	5
Aplicación web inventario de equipos	EXTREMO	5	9	9	8
Aplicaciones de ofimática	ALTO	5	3	9	6
Cliente de correo electrónico	ALTO	5	5	9	6
Computadores de funcionarios	MEDIO	5	5	5	5
Servidores	EXTREMO	9	9	9	9
Routers	EXTREMO	9	9	9	9

Cuadro 6 (Continuación)

Nombre	Riesgo	Confidencialidad	Integridad	Disponibilidad	Valor
Conexión a internet	EXTREMO	9	9	9	9
Red local	EXTREMO	9	9	9	9
Servicios de conectividad	EXTREMO	9	9	9	9
sistema de correo electrónico	EXTREMO	9	9	9	9
soporte Tic	ALTO	3	9	9	7
Colaboradores	MEDIO	5	5	5	5
Proveedor Tecnológico	MEDIO	5	5	5	5
Discos Duros	EXTREMO	9	9	9	9
Oficina	ALTO	5	5	9	6

Fuente. Metodología Magerit

7.1.4 Identificación y valoración de amenazas.

7.1.4.1 Amenazas.

Con la metodología Magerit se clasifica una serie de posibles amenazas las cuales se clasifican de la siguiente manera.

7.1.4.2 Identificar las Amenazas.

Es necesario la identificación de las amenazas que probablemente ocurran en los activos de MALLAMAS EPS INDÍGENA, para lo cual se describen las que se consideran más importantes:

“[N] Desastres

[N.1] Fuego

[N.2] Daños por agua

[N.*] Desastres

[I] De origen industrial.

[I.1] Fuego

[I.2] Daños por agua

[I.3] Contaminación mecánica

[I.4] Contaminación electromagnética

[I.5] Avería de origen físico o lógico

[I.6] Corte del suministro eléctrico

[I.7] Condiciones inadecuadas de temperatura o humedad

[I.8] Fallo de servicios de comunicaciones

[I.9] Interrupción de otros servicios y suministros

[I.10] Degradación de los soportes de almacenamiento de la información

[I.11] Emanaciones electromagnéticas

[E] Errores y fallos no intencionados.

[E.1] Errores de los usuarios

[E.2] Errores del administrador

[E.3] Errores de monitorización (log)

[E.4] Errores de configuración

[E.7] Deficiencias en la organización

[E.8] Difusión de software dañino

[E.9] Errores de [re-]encaminamiento

[E.10] Errores de secuencia

[E.14] Escapes de información

[E.15] Alteración accidental de la información

[E.18] Destrucción de información

[E.19] Fugas de información

[E.20] Vulnerabilidades de los programas (software)

[E.21] Errores de mantenimiento / actualización de programas(software)

[E.23] Errores de mantenimiento / actualización de equipos (hardware)

[E.24] Caída del sistema por agotamiento de recursos

[E.25] Pérdida de equipos

[E.28] Indisponibilidad del personal

[A] Ataques intencionados.

[A.3] Manipulación de los registros de actividad (log)

[A.4] Manipulación de la configuración

[A.5] Suplantación de la identidad del usuario

[A.6] Abuso de privilegios de acceso

[A.7] Uso no previsto

[A.8] Difusión de software dañino

[A.9] [Re-]encaminamiento de mensajes

[A.10] Alteración de secuencia

[A.11] Acceso no autorizado

[A.12] Análisis de tráfico

[A.13] Repudio

[A.14] Interceptación de información (escucha)

[A.15] Modificación deliberada de la información

[A.18] Destrucción de información

[A.19] Divulgación de información

[A.22] Manipulación de programas

[A.23] Manipulación de los equipos

[A.24] Denegación de servicio

[A.25] Robo

[A.26] Ataque destructivo

[A.27] Ocupación enemiga

[A.28] Indisponibilidad del personal

[A.29] Extorsión

[A.30] Ingeniería social (picaresca)" [27]

7.1.4.3 Valorar las amenazas

Brindar valoración a una vulnerabilidad en los activos es necesario hacer una evaluación en concordancia con su composición como, **la degradación** y **la probabilidad** de los activos versus a las amenazas.

Tabla 4 Valoración de probabilidad y degradación

Degradación	Valoración	Probabilidad	Valoración
5	muy alta	5	muy frecuente
4	Alta	4	frecuente
3	media	3	normal
2	Baja	2	poco frecuente
1	muy baja	1	muy poco frecuente

Fuente: Metodología Magerit

En el Cuadro 6 se establece la probabilidad de la vulnerabilidad por cada uno de los activos definidos, los cuales se valoran de acuerda a la escala anteriormente mencionada, de acuerdo con el modelo MAGERIT.

[27] Pilar. "MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos. Magerit 3.0. Madrid. Subdirección General de Información, Documentación y Publicaciones. 2012. P. 25-47 Disponible en: https://pilar.ccn-cert.cni.es/index.php/docman/documentos/2-magerit-v3-libro-ii-catalogo-de-elementos/file"

Cuadro 7 Valoración de la probabilidad

No.	Nombre del activo de información	Amenazas Metodología Magerit	Probabilidad de vulneración
1	Base de datos de inventario de Equipos	[E18] Destrucción de información	3
1	Base de datos de inventario de Equipos	[A6] Abuso de privilegios de acceso	4
2	Base de datos de solicitudes de soportes técnicos	[E18] Destrucción de información	3
2	Base de datos de solicitudes de soportes técnicos	[A6] Abuso de privilegios de acceso	2
3	Copias de Seguridad	[E2] Errores del administrador	5
3	Copias de Seguridad	[E3] Errores de monitorización (log)	4
4	Documentos de personal	[E18] Destrucción de información	3
4	Documentos de personal	[E1] Errores de los usuarios	3
5	Aplicaciones web osticket	[E21] Errores de mantenimiento / actualización de programas (software)	3
5	Aplicaciones web osticket	[I5] Avería de origen físico o lógico	3
6	Aplicación web inventario de equipos	[E21] Errores de mantenimiento / actualización de programas (software)	3
6	Aplicación web inventario de equipos	[I5] Avería de origen físico o lógico	3
7	Aplicaciones de ofimática	[E21] Errores de mantenimiento / actualización de programas (software)	4
7	Aplicaciones de ofimática	[E20] Vulnerabilidades de los programas (software)	4
8	Cliente de correo electrónico	[E8] Difusión de software dañino	4

Cuadro 7 (Continuación)

No.	Nombre del activo de información	Amenazas Metodología Magerit	Probabilidad de vulneración
8	Cliente de correo electrónico	[A11] Acceso no autorizado	3
9	Computadores de funcionarios	[I5] Avería de origen físico o lógico	3
9	Computadores de funcionarios	[I6] Corte del suministro eléctrico	4
10	Servidores	[I5] Avería de origen físico o lógico	3
10	Servidores	[I6] Corte del suministro eléctrico	4
11	Routers	[I5] Avería de origen físico o lógico	2
11	Routers	[I7] Condiciones inadecuadas de temperatura o humedad	3
12	Conexión a internet	[I8] Fallo de servicios de comunicaciones	2
12	Conexión a internet	[A12] Análisis de tráfico	3
13	Red local	[A11] Acceso no autorizado	3
13	Red local	[A12] Análisis de tráfico	3
14	Servicios de conectividad	[A24] Denegación de servicio	2
14	Servicios de conectividad	[E1] Errores de los usuarios	2
15	sistema de correo electrónico	[E1] Errores de los usuarios	4
15	sistema de correo electrónico	[A11] Acceso no autorizado	4
16	soporte Tic	[E7] Deficiencias en la organización	3
16	soporte Tic	[E28] Indisponibilidad del personal	3
17	Colaboradores	[A30] Ingeniería social (picaresca)	4
17	Colaboradores	[E7] Deficiencias en la organización	4
18	Proveedor Tecnológico	[E28] Indisponibilidad del personal	2
18	Proveedor Tecnológico	[E19] Fugas de información	3
19	Discos Duros	[I5] Avería de origen físico o lógico	2

Cuadro 7 (Continuación)

No.	Nombre del activo de información	Amenazas Metodología Magerit	Probabilidad de vulneración
19	Discos Duros	[E25] Pérdida de equipos	2
20	Oficina	[A11] Acceso no autorizado	3
20	Oficina	[N*] Desastres naturales	2

Fuente. Propia

7.1.5 Determinar el riesgo potencial.

La metodología Magerit "define como riesgo, a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia. El riesgo crece con el impacto y con la probabilidad"[28].

Para determinar el riesgo, se realiza la siguiente operación

"Valor Activo * Valor Probabilidad = Valor Riesgo."

Con este resultado es posible realizar la descripción de la escala que se va a utilizar para la valoración del riesgo, cuyo resultado es posible verlo reflejado en el cuadro.

[28] "Pilar. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método. Magerit 3.0. Madrid. Subdirección General de Información, Documentación y Publicaciones" "2012. P. 28 Disponible en: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html"

Cuadro 8 Calculo del Riesgo

Nombre del activo de información	Valoración Del Riesgo De Los Activos	Amenazas Metodología Magerit	Probabilidad de vulneración	Cálculo del riesgo neto
Base de datos de inventario de Equipos	22	[E18] Destrucción de información	3	66
Base de datos de inventario de Equipos	22	[A6] Abuso de privilegios de acceso	4	88
Base de datos de solicitudes de soportes técnicos	16	[E18] Destrucción de información	3	48
Base de datos de solicitudes de soportes técnicos	16	[A6] Abuso de privilegios de acceso	2	32
Copias de Seguridad	25	[E2] Errores del administrador	5	125
Copias de Seguridad	25	[E3] Errores de monitorización (log)	4	100
Documentos de personal	13	[E18] Destrucción de información	3	39
Documentos de personal	13	[E1] Errores de los usuarios	3	39
Aplicaciones web osticket	14	[E21] Errores de mantenimiento / actualización de programas (software)	3	42
Aplicaciones web osticket	14	[I5] Avería de origen físico o lógico	3	42
Aplicación web inventario de equipos	22	[E21] Errores de mantenimiento / actualización de programas (software)	3	66
Aplicación web inventario de equipos	22	[I5] Avería de origen físico o lógico	3	66

Cuadro 8 (Continuación)

Nombre del activo de información	Valoración Del Riesgo De Los Activos	Amenazas Metodología Magerit	Probabilidad de vulneración	Cálculo del riesgo neto
Aplicaciones de ofimática	16	[E21] Errores de mantenimiento / actualización de programas (software)	4	64
Aplicaciones de ofimática	16	[E20] Vulnerabilidades de los programas (software)	4	64
Cliente de correo electrónico	18	[E8] Difusión de software dañino	4	72
Cliente de correo electrónico	18	[A11] Acceso no autorizado	3	54
Computadores de funcionarios	15	[I5] Avería de origen físico o lógico	3	45
Computadores de funcionarios	15	[I6] Corte del suministro eléctrico	4	60
Servidores	25	[I5] Avería de origen físico o lógico	3	75
Servidores	25	[I6] Corte del suministro eléctrico	4	100
Routers	25	[I5] Avería de origen físico o lógico	2	50
Routers	25	[I7] Condiciones inadecuadas de temperatura o humedad	3	75
Conexión a internet	25	[I8] Fallo de servicios de comunicaciones	2	50
Conexión a internet	25	[A12] Análisis de tráfico	3	75
Red local	25	[A11] Acceso no autorizado	3	75

Cuadro 8 (Continuación)

Nombre del activo de información	Valoración Del Riesgo De Los Activos	Amenazas Metodología Magerit	Probabilidad de vulneración	Cálculo del riesgo neto
Red local	25	[A12] Análisis de tráfico	3	75
Servicios de conectividad	25	[A24] Denegación de servicio	2	50
Servicios de conectividad	25	[E1] Errores de los usuarios	2	50
sistema de correo electrónico	25	[E1] Errores de los usuarios	4	100
sistema de correo electrónico	25	[A11] Acceso no autorizado	4	100
soporte Tic	20	[E7] Deficiencias en la organización	3	60
soporte Tic	20	[E28] Indisponibilidad del personal	3	60
Colaboradores	15	[A30] Ingeniería social (picaresca)	4	60
Colaboradores	15	[E7] Deficiencias en la organización	4	60
Proveedor Tecnológico	15	[E28] Indisponibilidad del personal	2	30
Proveedor Tecnológico	15	[E19] Fugas de información	3	45
Discos Duros	25	[I5] Avería de origen físico o lógico	2	50
Discos Duros	25	[E25] Pérdida de equipos	2	50
Oficina	18	[A11] Acceso no autorizado	3	54
Oficina	18	[N*] Desastres naturales	2	36

Fuente. Propia

Para definir la criticidad es necesario tener en cuenta la escala de criticidad la cual se define de acuerdo con la figura 10.

Figura 10 Escala de Criticidad

VALORACIÓN DEL RIESGO			
	Nomenclatura	Categoría	Valoración
Valoracion del riesgo	C	Critico	21 a 25
	I	Importante	16 a 20
	A	Apreciable	10 a 15
	B	Bajo	5 a 9
	D	Despreciable	1 a 4

Fuente. Propia

De acuerdo con la escala anterior es posible definir la criticidad de acuerdo con el valor arrojado, por lo cual en cuadro 8 se puede evidenciar esta clasificación por cada activo.

Cuadro 9 Valoración de la Criticidad

No.	Nombre del activo de información	valoración del riesgo de los activos	amenazas metodología magerit	Niveles de aceptación del riesgo (N)	Probabilidad de vulneración	Cálculo del riesgo neto	Criticidad neta	Calificación de Gestión (C)	Riesgo residual(N/C)	Criticidad residual
1	Base de datos de inventario de Equipos	22	[E18] Destrucción de información	I	3	66	C	3	22	C
1	Base de datos de inventario de Equipos	22	[A6] Abuso de privilegios de acceso	I	4	88	C	1	88	C
2	Base de datos de solicitudes de soportes técnicos	16	[E18] Destrucción de información	I	3	48	C	3	16	I
2	Base de datos de solicitudes de soportes técnicos	16	[A6] Abuso de privilegios de acceso	M	2	32	C	3	11	A
3	Copias de Seguridad	25	[E2] Errores del administrador	I	5	125	C	1	125	C

Cuadro 9 (Continuidad)

No.	Nombre del activo de información	valoración del riesgo de los activos	amenazas metodología magerit	Niveles de aceptación del riesgo	Probabilidad de vulneración	Cálculo del riesgo neto	Criticidad neta	Calificación de Gestión (C)	Riesgo residual(N/C)	Criticidad residual
3	Copias de Seguridad	25	[E3] Errores de monitorización (log)	I	4	100	C	1	100	C
4	Documentos de personal	13	[E18] Destrucción de información	I	3	39	C	1	39	C
4	Documentos de personal	13	[E1] Errores de los usuarios	I	3	39	C	1	39	C
5	Aplicaciones web osticket	14	[E21] Errores de mantenimiento / actualización de programas (software)	M	3	42	C	3	14	A
5	Aplicaciones web osticket	14	[I5] Avería de origen físico o lógico	I	3	42	C	1	42	C

Cuadro 9 (Continuidad)

No.	Nombre del activo de información	valoración del riesgo de los activos	amenazas metodología magerit	Niveles de aceptación del riesgo	Probabilidad de vulneración	Cálculo del riesgo neto	Criticidad neta	Calificación de Gestión (C)	Riesgo residual(N/C)	Criticidad residual
6	Aplicación web inventario de equipos	22	[E21] Errores de mantenimiento / actualización de programas (software)	I	3	66	C	2	33	C
6	Aplicación web inventario de equipos	22	[I5] Avería de origen físico o lógico	I	3	66	C	1	66	C
7	Aplicaciones de ofimática	16	[E21] Errores de mantenimiento / actualización de programas (software)	I	4	64	C	3	21	C
7	Aplicaciones de ofimática	16	[E20] Vulnerabilidades de los programas (software)	I	4	64	C	3	21	C
8	Cliente de correo electrónico	18	[E8] Difusión de software dañino	I	4	72	C	1	72	C

Cuadro 9 (Continuidad)

No.	Nombre del activo de información	valoración del riesgo de los activos	amenazas metodología magerit	Niveles de aceptación del riesgo	Probabilidad de vulneración	Cálculo del riesgo neto	Criticidad neta	Calificación de Gestión (C)	Riesgo residual(N/C)	Criticidad residual
8	Cliente de correo electrónico	18	[A11] Acceso no autorizado	I	3	54	C	2	27	C
9	Computadores de funcionarios	15	[I5] Avería de origen físico o lógico	I	3	45	C	2	23	C
9	Computadores de funcionarios	15	[I6] Corte del suministro eléctrico	I	4	60	C	1	60	C
10	Servidores	25	[I5] Avería de origen físico o lógico	I	3	75	C	1	75	C
10	Servidores	25	[I6] Corte del suministro eléctrico	I	4	100	C	3	33	C
11	Routers	25	[I5] Avería de origen físico o lógico	I	2	50	C	1	50	C

Cuadro 9. (Continuidad)

No.	Nombre del activo de información	valoración del riesgo de los activos	amenazas metodología magerit	Niveles de aceptación del riesgo	Probabilidad de vulneración	Cálculo del riesgo neto	Criticidad neta	Calificación de Gestión (C)	Riesgo residual(N/C)	Criticidad residual
11	Routers	25	[I7] Condiciones inadecuadas de temperatura o humedad	I	3	75	C	1	75	C
12	Conexión a internet	25	[I8] Fallo de servicios de comunicaciones	I	2	50	C	3	17	I
12	Conexión a internet	25	[A12] Análisis de tráfico	I	3	75	C	1	75	C
13	Red local	25	[A11] Acceso no autorizado	I	3	75	C	3	25	C
13	Red local	25	[A12] Análisis de tráfico	I	3	75	C	1	75	C
14	Servicios de conectividad	25	[A24] Denegación de servicio	I	2	50	C	2	25	C
14	Servicios de conectividad	25	[E1] Errores de los usuarios	I	2	50	C	2	25	C

Cuadro 9. (Continuidad)

No.	Nombre del activo de información	valoración del riesgo de los activos	amenazas metodología magerit	Niveles de aceptación del riesgo	Probabilidad de vulneración	Cálculo del riesgo neto	Criticidad neta	Calificación de Gestión (C)	Riesgo residual(N/C)	Criticidad residual
15	sistema de correo electrónico	25	[E1] Errores de los usuarios	I	4	100	C	2	50	C
15	sistema de correo electrónico	25	[A11] Acceso no autorizado	I	4	100	C	2	50	C
16	soporte Tic	20	[E7] Deficiencias en la organización	I	3	60	C	1	60	C
16	soporte Tic	20	[E28] Indisponibilidad del personal	I	3	60	C	2	30	C
17	Colaboradores	15	[A30] Ingeniería social (picaresca)	I	4	60	C	1	60	C
17	Colaboradores	15	[E7] Deficiencias en la organización	I	4	60	C	2	30	C
18	Proveedor Tecnológico	15	[E28] Indisponibilidad del personal	M	2	30	C	3	10	B

Cuadro 9. (Continuidad)

No.	Nombre del activo de información	valoración del riesgo de los activos	amenazas metodología magerit	Niveles de aceptación del riesgo	Probabilidad de vulneración	Cálculo del riesgo neto	Criticidad neta	Calificación de Gestión (C)	Riesgo residual(N/C)	Criticidad residual
18	Proveedor Tecnológico	15	[E19] Fugas de información	I	3	45	C	3	15	A
19	Discos Duros	25	[I5] Avería de origen físico o lógico	I	2	50	C	1	50	C
19	Discos Duros	25	[E25] Pérdida de equipos	I	2	50	C	1	50	C
20	Oficina	18	[A11] Acceso no autorizado	I	3	54	C	1	54	C
20	Oficina	18	[N*] Desastres naturales	I	2	36	C	1	36	C

Fuente. Propia

Teniendo en cuenta la clasificación y su respectiva valoración del riesgo, y su criticidad, es necesario definir para todos estos activos los controles que se deben tener en cuenta para poder mitigar estos riesgos, por lo que en el siguiente capitulo, se definirá los controles necesarios en el marco de la norma ISO/27001

8 CONTROLES A LOS RIESGOS DE SEGURIDAD

Los controles en un sistema de gestión de seguridad son fundamentales, ya que estos ayudan a proteger la información de la entidad y su cumplimiento de acuerdo con el anexo técnico A, es obligatorio. Sin embargo, es importante establecer por cada entidad, cual preferiblemente va a aplicar, además es importante tener en cuenta que no solo involucra el área de tecnología sino también a recursos humanos, seguridad financiera, comunicaciones entre otros. Es este capitulo describiremos las actividades, que hay que desarrollar en los controles establecidos, por la norma.

8.1 CONTROLES A LOS RIESGOS POR ACTIVOS

De acuerdo con la norma ISO/27001, es posible determinar diferentes controles que se deben tomar, por lo cual en cuadro 9. se realizará la asignación del control pertinente por cada riesgo

8.2 PLAN DE ACCIÓN DE LOS CONTROLES A IMPLEMENTAR

De acuerdo con los controles definidos por el anexo técnico A, de la ISO 27001, por cada riesgo en el anterior capítulo en la presente tabla se realiza el plan de acción para poder desarrollar los controles solicitados, los cuales se realizan teniendo en cuenta las recomendaciones del framework de buenas prácticas NIST.

Cuadro 10 Plan de acción para llevar a cabo los controles ante los riesgos

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.5	POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN		
A.5.1.1	Políticas para la seguridad de la información	ID.GV-1	Creación de la política de seguridad, en los cuales se deben definir, los objetivos, el alcance, la cual debe estar alineada con la estrategia de los objetivos de la entidad, Es necesario que la política se encuentre aprobada y socializada por la alta dirección. Definir mediante qué circunstancias se actualiza y en cuanto tiempo, se recomienda realizarse de manera anual
A.5.1.2	Revisión de las políticas para la seguridad de la información.		
A.6	RESPONSABILIDAD Y ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN		
A.6.1	Organización interna		
A.6.1.1	Roles y responsabilidades para la seguridad de la información	ID.AM-6 ID.GV-2 PR.AT-2 PR.AT-3 PR.AT-4 PR.AT-5 DE.DP-1 RS.CO-1	Se deben definir los roles y responsables frente a la ciberseguridad. Los roles y las responsabilidades deben coordinarse y alinearse con las funciones y/o competencias, así mismo los proveedores, clientes, funcionarios, directores, deben comprender sus roles y responsabilidades, con el propósito que sean claros en el momento de detectar algún incidente. Es necesario definir un presupuesto formalmente para actividades de sensibilización de seguridad de información
A.6.1.2	Separación de deberes	PR.AC-4 PR.DS-5 RS.CO-3	Es necesario separar las funciones o deberes para que se evite accesos o modificaciones a los activos sin autorización, ni detección. Por este motivo se recomienda que la autorización de los eventos, este separado de quien los inicia

Cuadro 10. (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.6.1.3	Contacto con las autoridades	RS.CO-2	Establecer procedimientos mediante los cuales, se debe y a través de que medios notificar a las autoridades los eventos o incidentes de seguridad de información.
A.6.1.4	Contacto con grupos de interés especial	ID.RA-2	Inscribirse algún grupo, membresía o foro de interés de seguridad de información
A.6.1.5	Seguridad de la información en la gestión de proyectos.	PR.IP-2	Es necesario que para cada proyecto nuevo en sus fases se integre la seguridad de la información, con el propósito de identificar tempranamente los riesgos y sus respectivos controles.
A.6.2	**Dispositivos móviles y teletrabajo**		
A.6.2.1	**Política para dispositivos móviles**		Establecer la política de seguridad, para dispositivos móviles de propiedad personal, en donde se establezca acuerdos de confidencialidad al acceso de la información de la entidad, en donde se contemplen y se reconozcan los deberes de protección física, actualización de software, desistir de la propiedad de los datos de empresa, permitir el borrado de datos por parte de la entidad de manera remota, en caso de pérdida o robo o cuando ya no se tenga autorización para utilizar el servicio.

Cuadro 10. (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.6.2.2	**Teletrabajo**	PR.AC-3	Establecer políticas de seguridad para personas que realicen teletrabajo, en donde se debe establecer diferentes aspectos como: a) La seguridad física existente en el sitio del teletrabajo b) Los requisitos de seguridad de las comunicaciones, teniendo en cuenta la necesidad de acceso remoto a los sistemas internos de la organización, la sensibilidad de la información a la que se tendrá acceso y que pasará a través del enlace de comunicación y la sensibilidad del sistema interno c) El suministro de acceso al escritorio virtual, que impide el procesamiento y almacenamiento de información en equipo de propiedad privada d) La amenaza de acceso no autorizado a información o a recursos, por parte de otras personas que usan el mismo equipo, por ejemplo, familia y amigos e) El uso de redes domésticas y requisitos o restricciones sobre la configuración de servicios de red inalámbrica e) Acuerdos de licenciamiento de software de tal forma que las organizaciones puedan llegar a ser responsables por el licenciamiento de software de los clientes en estaciones de trabajo de propiedad de los empleados o de usuarios externos f) Requisitos de firewall y de protección contra software malicioso

			Las directrices y acuerdos que se consideren deberían incluir g) El suministro de equipo adecuado y de muebles de almacenamiento para las actividades de teletrabajo, cuando no se permite el uso del equipo de propiedad privada que no está bajo el control de la organización h) Una definición del trabajo permitido, las horas de trabajo, la clasificación de la información que se puede mantener, y los sistemas y servicios internos a los que el teletrabajador está autorizado a acceder; i) El suministro de equipos de comunicación adecuados, incluidos los métodos para asegurar el acceso remoto j) La revocación de la autoridad y de los derechos de acceso, y la devolución de los equipos cuando las actividades del teletrabajo finalicen

Cuadro 10. (Continuidad)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.7	**SEGURIDAD DE LOS RECURSOS HUMANOS**		
A.7.1	**Antes de asumir el empleo**		
A.7.1.1	**Selección**	PR.DS-5 PR.IP-11	En el procedimiento de contratación tanto del personal como de proveedores, es necesario se tenga en cuenta todo lo relacionado con la privacidad, la protección de datos personales, y la legislación laboral y llevar a cabo todo el proceso de selección de personal implementado en la empresa, esto es la verificación de referencias personales, académicas, comerciales, laborales, crediticias, antecedentes pénales, pruebas sicotécnicas y pruebas relacionadas con el cargo. Cuando se maneje información crítica o muy confidencial, la entidad debe considerar verificaciones más detalladas, como estudio de seguridad, polígrafo, visitas domiciliarias etc.. Para contratistas o proveedores se debe garantizar proceso de selección, en donde se especifique responsabilidades de la selección y los procedimientos de notificación. La recolección de toda la información de este procedimiento y el manejo de esta debe darse de acuerdo con la ley de datos personales.

Cuadro 10. (continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.7.1.2	**Términos y condiciones del empleo**	PR.DS-5	Cuando se seleccione personal se debe informar durante el proceso de vinculación los roles y responsabilidades de seguridad de la información. En los contratos de empleados y contratistas que tengan acceso a información confidencial agregar una cláusula de confidencialidad y no divulgación, protección de datos, ética, uso apropiado de los equipos e instalaciones de la entidad. Las acciones por tomar si no se tiene en cuenta los requisitos de seguridad de la entidad. (Ver control 7.2.3) y las responsabilidades al finalizar el contrato. (Ver control 7.3.1).
A.7.2	**Durante la vigencia Contractual**		

Cuadro 10. (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.7.2.1	**Responsabilidades de la dirección**	ID.GV-2	Los funcionarios deben estar debidamente informados sobre sus roles y responsabilidades de seguridad de la información, antes de que se les otorgue el acceso a información o sistemas de información confidenciales. Lograr que se tome conciencia sobre seguridad de la información pertinente a sus roles y responsabilidades dentro de la entidad y estén motivados para cumplir con las políticas. Tengan continuamente las habilidades y calificaciones apropiadas y reciban capacitación en forma regular. Contar con un canal para reporte anónimo de incumplimiento de las políticas o procedimientos de seguridad de la información a través de denuncias internas En los contratos de empleados y contratistas que tengan acceso a información confidencial agregar una cláusula de confidencialidad y no divulgación, protección de datos, ética, uso apropiado de los equipos e instalaciones de la entidad. Las acciones por tomar si no se tiene en cuenta los requisitos de seguridad de la entidad. (Ver control 7.2.3) y las responsabilidades al finalizar el contrato. (Ver control 7.3.1).

Cuadro 10. (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.7.2.2	**Toma de conciencia, educación y formación en la seguridad de la información.**	PR.AT-1 PR.AT-2 PR.AT-3 PR.AT-4 PR.AT-5	Realizar un plan de comunicación, sensibilización y capacitación, en donde se realice el respectivo registro de evidencias, los cuales deben estar revisados y aprobados por la alta Dirección. En este plan es necesario que contemple las siguientes ítems Desarrollo de campañas, elaboración de folletos y boletines. Inducción a los nuevos empleados y contratistas sobre la sensibilización en SI. Realizar y establecer cada cuanto se actualizan los programas de toma de conciencia. Registro de asistencia al programa y los temas impartidos Incluir en los temas de toma de conciencia los procedimientos básicos de seguridad de la información (tales como el reporte de incidentes de seguridad de la información) y los controles de línea base (tales como la seguridad de las contraseñas, los controles del software malicioso, y los escritorios limpios).
A.7.2.3	**Proceso disciplinario**		Definir los procesos disciplinarios que se sigue cuando ha ocurrido una violación a la seguridad de la información, así como quien y como se determina la sanción al infractor, la cual debe darse a conocer cuando se realice la vinculación al personal.
A.7.3	**Terminación y cambio de empleo**		

Cuadro 10. (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.7.3.1	**Terminación o cambio de responsabilidades de empleo**	PR.DS-5 PR.IP-11	Revisar los acuerdos de confidencialidad, verificando que deben acordar que después de terminada la relación laboral o contrato seguirán vigentes por un periodo de tiempo.
A.8	**GESTIÓN DE ACTIVOS**		
A.8.1	**Responsabilidad por los activos**		
A.8.1.1	**Inventario de activos**	ID AM-1 ID AM-2 ID.AM-5	Realizar el inventario de los activos de la información, los cuales deben ser aprobados por la alta dirección, en donde se debe contemplar lo siguiente: registro de las actualizaciones. Definición de los propietarios de los activos. Definir el encargado de la actualización y revisión del inventario de activos, además de la periodicidad de la revisión.
A.8.1.2	**Propiedad de los activos**	ID AM-1 ID AM-2	Definir el procedimiento en donde se contemple la asignación oportuna de la propiedad de los activos. cuando estos sean creados o cuando son entregados a la Entidad El propietario de los activos tiene la responsabilidad de asegurarse de que los activos estén inventariados, asegurarse de que los activos están clasificados y protegidos apropiadamente, definir y revisar periódicamente las restricciones y clasificaciones de acceso a activos importantes, teniendo en cuenta las políticas de control de acceso aplicables, asegurarse del manejo apropiado del activo cuando es eliminado o destruido

Cuadro 10. (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.8.1.3	**Uso aceptable de los activos**		Pregunte por la política, procedimiento, directriz o lineamiento que defina el uso aceptable de los activos, verifique que es conocida por los empleados y usuarios de partes externas que usan activos de la Entidad o tienen acceso a ellos.
A.8.1.4	**Devolución de activos**	PR.IP-11	Revisar y de ser necesario crear los procedimientos y directrices relativas a los controles de seguridad de la información durante la terminación de la relación laboral, en el momento de la devolución de los activos de información (equipos, llaves, documentos , datos, sistemas) , eliminación de los derechos de acceso, En caso de que un funcionario o tercero sea el dueño del activo es necesario asegurar la transferencia de la información a la Entidad y el borrado seguro de la información de la misma. En caso en que un empleado o usuario de una parte externa posea conocimientos que son importantes para las operaciones regulares, esa información se debería documentar y transferir a la Entidad. Durante el período de notificación de la terminación, la Entidad debería controlar el copiado no autorizado de la información pertinente por parte de los empleados o contratistas que han finalizado el empleo.
A.8.2	**Clasificación de la información**		

Cuadro 10. (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.8.2.1	**Clasificación de la información**		Documentar el procedimiento mediante el cual se clasifican los activos de información en donde se evidencie las convenciones y criterios de clasificación sean claros; Que se defina cada cuanto debe revisarse la clasificación de estos y si esta debiera valorarse analizando la confidencialidad, integridad y disponibilidad.
A.8.2.2	**Etiquetado de la información**	PR.DS-5 PR.PT-2	Definir el procedimiento para el etiquetado de la información en donde se refleje el esquema de clasificación establecido, Que las etiquetas se puedan reconocer fácilmente y que los empleados y contratistas conocen el procedimiento de etiquetado
A.8.2.3	**Manejo de activos**	PR.DS-1 PR.DS-2 PR.DS-3 PR.DS-5 PR.IP-6 PR.PT-2	Definir los procedimientos para el manejo, procesamiento, almacenamiento y comunicación de información de conformidad con su clasificación. en donde se debe contemplar la restricciones de acceso, Registro formal de los receptores autorizados de los activos, la protección de copias de información temporal o permanente, Almacenamiento de los activos de TI de acuerdo con las especificaciones de los fabricantes y que la información almacenada (at rest) y en tránsito debe ser protegida mediante cifrado o token.
A.8.3	**Manejo de medios**		

Cuadro 10. (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.8.3.1	**Gestión de medio removibles**	PR.DS-3 PR.IP-6 PR.PT-2	Definir procedimientos para la gestión de medios removibles, en donde se considere: Si ya no se requiere, el contenido de cualquier medio reusable que se vaya a retirar de la organización se debe remover de forma que no sea recuperable; Que cuando resulte necesario y práctico, se debe solicitar autorización para retirar los medios de la organización, y se debe llevar un registro de dichos retiros con el fin de mantener un rastro de auditoría; Si la confidencialidad o integridad de los datos se consideran importantes, se deben usar técnicas criptográficas para proteger los datos que se encuentran en los medios removibles; Se deben guardar varias copias de los datos valiosos en medios separados, para reducir aún más el riesgo de daño o pérdida casuales de los datos; Sólo se deben habilitar unidades de medios removibles si hay una razón de valida asociada a los procesos la Entidad para hacerlo En donde hay necesidad de usar medios removibles, se debería hacer seguimiento a la transferencia de información a estos medios mediante herramientas como los DLP
A.8.3.2	**Disposición de los medios**	PR.DS-3 PR.IP-6	Definir el procedimiento en donde se garantice que los medios a desechar o donar, no contienen información confidencial que pueda ser consultada y copiada por personas no autorizadas.

Cuadro 10. (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.8.3.3	**Transferencia de medios físicos**	PR.DS-3 PR.PT-2	Definir el procedimiento mediante el cual se realice la protección de medios que contienen información durante el transporte. en donde se contemple: a) El uso de un transporte o servicios de mensajería confiables. b) Procedimientos para verificar la identificación de los servicios de mensajería. c)Garantizar el embalaje, el cual debe proteger el contenido contra cualquier daño físico que pudiera presentarse durante el tránsito, y de acuerdo con las especificaciones de los fabricantes, por ejemplo, protección contra cualquier factor ambiental que pueda reducir la eficacia de la restauración del medio, tal como exposición al calor, humedad o campos electromagnéticos d)Registros que dejen evidencia del transporte donde se identifique el contenido de los medios, la protección aplicada, al igual que los tiempos de transferencia a los responsables durante el transporte, y el recibo en su destino.
A.9	**CONTROL DE ACCESO**		
A.9.1	**Requisitos del negocio para el control de acceso**		

Cuadro 10. (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.9.1.1	**Política de control de acceso**	PR.DS-5	Creación de la política donde contenga lo siguiente: a) los requisitos de seguridad para las aplicaciones del negocio; b) las políticas para la divulgación y autorización de la información, y los niveles de seguridad de la información y de clasificación de la información; c) la coherencia entre los derechos de acceso y las políticas de clasificación de información de los sistemas y redes; d) la legislación pertinente y cualquier obligación contractual concerniente a la limitación del acceso a datos o servicios; e) la gestión de los derechos de acceso en un entorno distribuido y en red, que reconoce todos los tipos de conexiones disponibles; f) la separación de los roles de control de acceso, (solicitud de acceso, autorización de acceso, administración del acceso); g) los requisitos para la autorización formal de lassolicitudes de acceso; h) los requisitos para la revisión periódica de los derechos de acceso; i) el retiro de los derechos de acceso; j) el ingreso de los registros de todos los eventos significativos concernientes al uso y gestión de identificación de los usuarios, e información de autenticación secreta, en el archivo permanente; k) los roles de acceso privilegiado

Cuadro 10. (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.9.1.2	**Acceso a redes y a servicios en red**	PR.AC-4 PR.DS-5 PR.PT-3	Creación de la política relacionada con el uso de redes y de servicios de red y verificar que incluya: a) las redes y servicios de red a los que se permite el acceso b) los procedimientos de autorización para determinar a quién se permite el acceso a qué redes y servicios de red c) los controles y procedimientos de gestión para proteger el acceso a las conexiones de red y a los servicios de red d) los medios usados para acceder a las redes y servicios de red (uso de VPN o redes inalámbricas) e) los requisitos de autenticación de usuarios para acceder a diversos servicios de red f) el seguimiento del uso de servicios de red.
A.9.2	**Gestión de acceso de usuarios**		
A.9.2.1	**Registro y cancelación del registro de usuarios**	PR.AC-1	Realizar el procedimiento para la gestión y la identificación de los usuarios en donde se contemple: a) Identificaciones únicas para los usuarios, que les permita estar vinculados a sus acciones y mantener la responsabilidad por ellas. b) deshabilitar o retirar inmediatamente las identificaciones de los usuarios que han dejado la organización c) identificar y eliminar o deshabilitar periódicamente las identificaciones de usuario redundantes d) asegurar que las identificaciones de usuario redundantes no se asignen a otros usuarios.

Cuadro 10. (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.9.2.2	**Suministro de acceso de usuarios**	PR.AC-1	Definir el procedimiento mediante el cual se asigna o revoca los derechos de acceso otorgados a las identificaciones de usuario las cuales deben incluir: a) obtener la autorización del propietario del sistema de información o del servicio para el uso del sistema de información o servicio; b) verificar que el nivel de acceso otorgado es apropiado a las políticas de acceso y es coherente con otros requisitos, tales como separación de deberes; c) asegurar que los derechos de acceso no estén activados antes de que los procedimientos de autorización estén completos; d) mantener un registro central de los derechos de acceso suministrados a una identificación de usuario para acceder a sistemas de información y servicios; e) adaptar los derechos de acceso de usuarios que han cambiado de roles o de empleo, y retirar o bloquear inmediatamente los derechos de acceso de los usuarios que han dejado la organización; f) revisar periódicamente los derechos de acceso con los propietarios de los sistemas de información o servicios.

Cuadro 10. (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.9.2.3	**Gestión de derechos de acceso privilegiado**	PR.AC-4 PR.DS-5	Revisión de la asignación de derechos de acceso privilegiado a través de un proceso de autorización formal de acuerdo con la política de control de acceso pertinente. el proceso debe incluir los siguientes pasos: a) Identificar los derechos de acceso privilegiado asociados con cada sistema o proceso, (sistema operativo, sistema de gestión de bases de datos, y cada aplicación) y los usuarios a los que es necesario asignar b) definir o establecer los derechos de acceso privilegiado a usuarios con base en la necesidad de uso y caso por caso, alineada con la política de control de acceso; c) mantener un proceso de autorización y un registro de todos los privilegios asignados. Sólo se debe suministrar derechos de acceso cuando el proceso de autorización esté completo d) definir los requisitos para la expiración de los derechos de acceso privilegiado e) establecer los derechos de acceso privilegiado a través de una identificación de usuario diferente de la usada para las actividades regulares del negocio. Las actividades regulares del negocio no se ejecutan desde una identificación privilegiada f) tener las competencias de los usuarios con derechos de acceso privilegiado y su revisión periódica para verificar si están en línea con sus deberes g) establecer y mantener procedimientos genéricos para evitar el uso no autorizado de identificaciones de usuario de administración genérica, de acuerdo con las capacidades de configuración del sistema h) establecer la confidencialidad de la información de autenticación secreta, para las identificaciones de usuario de administración genérica, cuando se comparta (cambiar las contraseñas con frecuencia, y cuando un usuario privilegiado ha dejado el trabajo o cambia de trabajo, comunicarlas entre los usuarios privilegiados con los mecanismos apropiados).

Cuadro 10. (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.9.2.4	**Gestión de información de autenticación secreta de usuarios**	PR.AC-1	Definir el procedimiento en el cual se establezca: a) La firma de una declaración para mantener confidencial la información de autenticación secreta personal, y mantener la información de autenticación secreta del grupo (cuando es compartida) únicamente dentro de los miembros del grupo, esta declaración firmada se puede incluir en los términos y condiciones del empleo para todos los que los usuarios b) estipular que todos los usuarios deben mantener su propia información de autenticación secreta, y se les suministra una autentificación secreta temporal segura, que se obligue a cambiar al usarla por primera vez c) establecer procedimientos para verificar la identidad de un usuario antes de proporcionarle la nueva información de autenticación secreta de reemplazo o temporal d) definir que la información de autenticación secreta temporal se suministra a los usuarios de una manera segura y se evitar utilizar partes externas o de mensajes de correo electrónico no protegidos (texto claro) e) establecer que la información de autenticación secreta temporal es única para un individuo y no es fácil de adivinar f) definir que los usuarios deben acusar recibo de la información de autenticación secreta g) establecer que la información de autenticación secreta por defecto, del fabricante, se modifica después de la instalación de los sistemas o software.

Cuadro 10. (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.9.2.5	**Revisión de los derechos de acceso de usuarios**		Definir los procedimientos de revisión de los derechos de acceso en donde se establezca: a) Examinar los derechos de acceso de los usuarios periódicamente y después de cualquier cambio, promoción, cambio a un cargo a un nivel inferior, o terminación del empleo; b) Establecer que los derechos de acceso de usuario se revisan y reasignan cuando pasan de un rol a otro dentro de la misma organización; c) Definir las autorizaciones para los derechos de acceso privilegiado y revisar periódicamente; d) Verificar las asignaciones de privilegios periódicamente, para asegurar que no se hayan obtenido privilegios no autorizados; e) Revisar y registrar los cambios a las cuentas privilegiadas periódicamente.
A.9.2.6	**Retiro o ajuste de los derechos de acceso**		Definir el procedimiento mediante el cual se revise los derechos de acceso a la información y a los activos asociados con instalaciones de procesamiento de información, antes de que el empleo termine o cambie, dependiendo de la evaluación de factores de riesgo que incluya: a) Terminación o cambio lo inicia el empleado, el usuario de la parte externa o la dirección, y la razón de la terminación b) Revisar las responsabilidades actuales del empleado, el usuario de la parte externa o cualquier otro usuario c) Verificar el valor de los activos accesibles en la actualidad. Cuando se piense en cancelar un contrato a un empleado hay que extraer la información antes de comunicárselo para evitar acciones deliberadas por parte de este. Igualmente, cuando el empleado pasa la carta de renuncia hay que hacer la respectiva copia de la información.
A.9.3	**Responsabilidades de los usuarios**		

Cuadro 10. (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.9.3.1	**Uso de información de autenticación secreta**	PR.AC-1	Definir el procedimiento de notificación a usuarios el cual debe incluir: a) Mantener la confidencialidad de la información de autenticación secreta, asegurándose de que no sea divulgada a ninguna otra parte, incluidas las personas con autoridad b) Evitar llevar un registro (en papel, en un archivo de software o en un dispositivo portátil) de autenticación secreta, a menos que se pueda almacenar en forma segura y que el método de almacenamiento haya sido aprobado (una bóveda para contraseñas) c) Cambiar la información de autenticación secreta siempre que haya cualquier indicio de que se pueda comprometer la información d) Definir que cuando se usa contraseñas como información de autenticación secreta, se debe seleccionar contraseñas seguras con una longitud mínima suficiente que: Sean fáciles de recordar; No estén basadas en algo que otra persona pueda adivinar fácilmente u obtener usando información relacionada con la persona, (nombres, números de teléfono y fechas de nacimiento, etc.), que no sean vulnerables a ataques de diccionario (es decir, no contienen palabras incluidas en los diccionarios); estén libres de caracteres completamente numéricos o alfabéticos idénticos consecutivos; si son temporales, cambiarlos la primera vez que se ingrese; no compartir información de autenticación secreta del usuario individual establecer una protección apropiada de contraseñas cuando se usan éstas como información de autenticación secreta en procedimientos de ingreso automatizados, y estén almacenadas; no usar la misma información de autenticación secreta para propósitos de negocio y otros diferentes de estos.

Cuadro 10. (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.9.4	**Control de acceso a sistemas y aplicaciones**		
A.9.4.1	**Restricción de acceso a la información**	PR.AC-4 PR.DS-5	Definir procedimientos o lineamientos mediante los cuales se den restricciones de acceso a través de la aplicación individual del negocio y de acuerdo con la política de control de acceso definida; que incluya: a) suministrar menús para controlar el acceso a las funciones de sistemas de aplicaciones b) controlar a qué datos puede tener acceso un usuario particular; c) controlar los derechos de acceso de los usuarios, (a leer, escribir, borrar y ejecutar); d) controlar los derechos de acceso de otras aplicaciones; e) limitar la información contenida en los elementos de salida; f) proveer controles de acceso físico o lógico para el aislamiento de aplicaciones, datos de aplicaciones o sistemas críticos.

Cuadro 10. (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.9.4.2	**Procedimiento de ingreso seguro**	PR.AC-1	Definir el procedimiento de ingreso que debe incluir: a) No visualizar los identificadores del sistema o de la aplicación sino hasta que el proceso de ingreso se haya completado exitosamente b) visualizar una advertencia general acerca de que sólo los usuarios autorizados pueden acceder al computador c) evitar los mensajes de ayuda durante el procedimiento de ingreso, que ayudarían a un usuario no autorizado d) validar la información de ingreso solamente al completar todos los datos de entrada. ante una condición de error, el sistema no debe indicar qué parte de los datos es correcta o incorrecta e) proteger contra intentos de ingreso mediante fuerza bruta f) llevar un registro con los intentos exitosos y fallidos g) declarar un evento de seguridad si se detecta un intento potencial o una violación exitosa de los controles de ingreso h) visualizar la información al terminar un ingreso seguro, como el registro de la fecha y la hora del ingreso previo exitoso, registrar los detalles de cualquier intento de ingreso no exitoso desde el último ingreso exitoso. i) no visualizar una contraseña que se esté ingresando j) no transmitir contraseñas en un texto claro en una red k) terminar sesiones inactivas después de un período de inactividad definido, especialmente en lugares de alto riesgo tales como áreas públicas o externas por fuera de la gestión de seguridad de la organización o en dispositivos móviles l) restringir los tiempos de conexión para brindar seguridad adicional para aplicaciones de alto riesgo y para reducir la ventana de oportunidad para acceso no autorizado.

Cuadro 10. (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.9.4.3	**Sistema de gestión de contraseñas**	PR.AC-1	Definir el procedimiento o lineamiento para el sistema de gestión de contraseñas en donde se incluya: a) Cumplir el uso de identificaciones y contraseñas de usuarios individuales para mantener la rendición de cuentas b) permitir que los usuarios seleccionen y cambien sus propias contraseñas e incluyan un procedimiento de confirmación para permitir los errores de entrada c) Exigir por que se escojan contraseñas de calidad d) Forzar a los usuarios cambiar sus contraseñas cuando ingresan por primera vez; e) Exigir por que se cambien las contraseñas en forma regular, según sea necesario: f) llevar un registro de las contraseñas usadas previamente, e impedir su reusó g) no visualizar contraseñas en la pantalla cuando se está ingresando h) almacenar los archivos de las contraseñas separadamente de los datos del sistema de aplicaciones i) almacenar y transmitir las contraseñas en forma protegida.

Cuadro 10. (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.9.4.4	**Uso de programas utilitarios privilegiados**	PR.AC-4 PR.DS-5	Definir las directrices para el uso de programas utilitarios con la capacidad de anular los controles de sistemas y de aplicaciones, que incluyan. a) utilizar procedimientos de identificación, autenticación y autorización para los programas utilitarios b) separar los programas utilitarios del software de aplicaciones c) limitar el uso de programas utilitarios al número mínimo práctico de usuarios confiables y autorizados d) autorizar el uso adhoc de programas utilitarios e) limitar la disponibilidad de los programas utilitarios f) registrar el uso de los programas utilitarios g) definir y documentar los niveles de autorización para los programas utilitarios h) retirar o deshabilitar todos los programas utilitarios innecesarios i) No poner a disposición los programas utilitarios a los usuarios que tengan acceso a aplicaciones en sistemas en donde se requiera la separación de deberes.

Cuadro 10. (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.9.4.5	**Control de acceso a códigos fuente de programas**	PR.DS-5	Definir el procedimiento para la gestión de códigos fuente de los programas, que incluya: a) Definir en donde sea posible, las librerías de fuentes de programas no se deben mantener en los sistemas operativos b) Gestionar los códigos fuente de los programas y las librerías de las fuentes de los programas se debería hacer de acuerdo con procedimientos establecidos c) Establecer que el personal de soporte deben tener acceso restringido a las librerías de las fuentes de los programas d) Definir que la actualización de las librerías de fuentes de programas y elementos asociados, y la entrega de fuentes de programas a los programadores sólo se deben hacer una vez que se haya recibido autorización apropiada e) Establecer que los listados de programas se deben mantener en un entorno seguro f) Conservar un registro de auditoría de todos los accesos a la librerías de fuentes de programas; g) Mantener y copiar las bibliotecas de fuentes de programas a través de procedimientos estrictos de control de cambios.
A.10	**CRIPTOGRAFÍA**		
A.10.1	**Controles criptográficos**		

Cuadro 10. (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.10.1.1	**Política sobre el uso de controles criptográficos**		Definir la política sobre el uso de la criptográfica, en el momento que se requiera en donde debe incluir: a)El establecimiento del enfoque de la dirección con relación al uso de controles criptográficos en toda la organización, incluyendo los principios generales bajo los cuales se deben proteger la información del negocio b) realizar una valoración de riesgos, que identifique el nivel de protección requerida, teniendo en cuenta el tipo, fortaleza y calidad del algoritmo de encriptación requerido. c) utilizar la encriptación para la protección de información transportada por dispositivos de encriptación móviles o removibles, o a través de líneas de comunicación d) gestionar las llaves y los métodos para la protección de llaves criptográficas y la recuperación de información encriptada, en el caso de llaves perdidas, llaves cuya seguridad está comprometida, o que están dañadas e) establecer roles y responsabilidades, quién es responsable por: la implementación de la política, la gestión de llaves, incluida la generación de llaves; f) establecer las normas que se van a adoptar para la implementación efectiva en toda la organización (procesos del negocio) g) definir el impacto de usar información encriptada en los controles que dependen de la inspección del contenido.

Cuadro 10. (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.10.1.2	**Gestión de llaves**		Definir la gestión de llaves que debe estar basado en un grupo establecido de normas, procedimientos y métodos seguros para: a) Generar llaves para diferentes sistemas criptográficos y diferentes aplicaciones b) Generar y obtener certificados de llaves públicas; c) Distribuir llaves a las entidades previstas, incluyendo la forma de recibir y activar las llaves d) Almacenar las llaves, incluyendo la forma en que los usuarios autorizados obtienen acceso a ellas e) Cambiar o actualizar las llaves, incluyendo las reglas sobre cuándo se deben cambiar y cómo hacerlo f) Dar tratamiento a las llaves cuya seguridad está comprometida g) Revocar las llaves, incluyendo la forma de retirarlas o desactivarlas, cuando la seguridad de las llaves ha estado comprometida, o cuando un usuario deja la organización h) Recuperar las llaves que estén perdidas o dañadas i) Hacer copias de respaldo de las llaves o archivarlas; j) Destruir las llaves k) Registrar y auditar las actividades relacionadas con gestión de llaves.
A.11	**SEGURIDAD FÍSICA Y DEL ENTORNO**		
A.11.1	**Áreas seguras**		

Cuadro 10. (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.11.1.1	**Perímetro de seguridad física**	PR.AC-2	Establecer las directrices relacionadas con los perímetros de seguridad física: a) Definir los perímetros de seguridad, y el emplazamiento y fortaleza de cada uno de los perímetros deben depender de los requisitos de seguridad de los activos dentro del perímetro y de los resultados de una valoración de riesgos; b) Establecer los perímetros de una edificación o sitio que contenga instalaciones de procesamiento de la información debe ser físicamente seguros; el techo exterior, las paredes y el material de los pisos del sitio deben ser de construcción sólida, y todas las paredes externas deben estar protegidas adecuadamente contra acceso no autorizado con mecanismos de control (barras, alarmas, cerraduras); las puertas y ventanas deben estar cerradas con llave cuando no hay supervisión, y se debe considerar protección externa para ventanas, particularmente al nivel del suelo c) Definir un área de recepción con vigilancia u otro medio para controlar el acceso físico al sitio o edificación; el acceso a los sitios y edificaciones debe estar restringido únicamente para personal autorizado d) Establecer cuando sea aplicable y construir barreras físicas para impedir el acceso físico no autorizado y la contaminación ambiental e) Establecer que todas las puertas contra incendio en un perímetro de seguridad deben tener alarmas, estar monitoreadas y probadas junto con las paredes, para establecer el nivel requerido de resistencia de acuerdo con normas regionales, nacionales e internacionales adecuadas deben funcionar de manera segura de

			acuerdo al código local de incendios f) Instalar sistemas adecuados para detección de intrusos de acuerdo con normas nacionales, regionales o internacionales y se deben probar regularmente para abarcar todas las puertas externas y ventanas accesibles; las áreas no ocupadas deben tener alarmas en todo momento; también deben abarcar otras áreas, tales como las salas de cómputo o las salas de comunicaciones g) Establecer que las instalaciones de procesamiento de información gestionadas por la organización deben estar separadas físicamente de las gestionadas por partes externas.

Cuadro 10. (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.11.1.2	**Controles de acceso físicos**	PR.AC-2 PR. MA-1	Establecer los controles de acceso físico y las siguientes directrices: a) Tener un registro de la fecha y hora de entrada y salida de los visitantes, y todos los visitantes deben ser supervisados a menos que su acceso haya sido aprobado previamente; solo se les debe otorgar acceso para propósitos específicos autorizados y se deben emitir instrucciones sobre los requisitos de seguridad del área y de los propósitos de emergencia. La identidad de los visitantes se deben autenticar por los medios apropiados b) Establecer que el acceso a las áreas en las que se procesa o almacena información confidencial se debería restringir a los individuos autorizados solamente mediante la implementación de controles de acceso apropiados, (mediante la implementación de un mecanismo de autenticación de dos factores, tales como una tarjeta de acceso y un PIN secreto) c) Mantener y hacer seguimiento de un libro de registro (physical log book) físico o un rastro de auditoría electrónica de todos los accesos d) Definir que todos los empleados, contratistas y partes externas deben portar algún tipo de identificación visible, y se deben notificar de inmediato al personal de seguridad si se encuentran visitantes no acompañados, y sin la identificación visible e) Establecer que el personal de servicio de soporte de la parte externa se le debería otorgar acceso restringido a áreas seguras o a instalaciones de procesamiento de información confidencial solo cuando se requiera; este acceso se deben autorizar y se le debe hacer seguimiento f) Definir los derechos de acceso a áreas seguras se deben revisar y actualizar regularmente, y revocar cuando sea necesario.

Cuadro 10. (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.11.1.3	**Seguridad de oficinas, recintos e instalaciones.**		Establecer las siguientes directrices relacionadas con la seguridad a oficinas, recintos e instalaciones: a) Establecer que las instalaciones clave deben estar ubicadas de manera que se impida el acceso del público b) Definir donde sea aplicable, las edificaciones deben ser discretas y dar un indicio mínimo de su propósito, sin señales obvias externas o internas, que identifiquen la presencia de actividades de procesamiento de información c) Establecer que las instalaciones deben estar configuradas para evitar que las actividades o información confidenciales sean visibles y audibles desde el exterior. El blindaje electromagnético también se debe ser el apropiado d) Definir los directorios y guías telefónicas internas que identifican los lugares de las instalaciones de procesamiento de información confidencial no deben ser accesibles a ninguna persona no autorizada.
A.11.1.4	**Protección contra amenazas externas y ambientales.**	ID.BE-5 PR.AC-2 PR.IP-5	Establecer la protección frente a las posibles amenazas externas y ambientales.
A.11.1.5	**Trabajo en áreas seguras.**		Se deben definir directrices frente al trabajo en área segura: a) Establecer que el personal solo debe conocer de la existencia de un área segura o de actividades dentro de un área segura, con base en lo que necesita conocer; b) definir que el trabajo no supervisado en áreas seguras se debe evitar tanto por razones de seguridad como para evitar oportunidades para actividades malintencionadas c) establecer que las áreas seguras vacías deben estar cerradas con llave y se revisan periódicamente d) no se permite el ingreso y uso de equipo fotográfico, de video, audio u otro equipo de grabación, tales como cámaras en dispositivos móviles, a menos que se cuente con autorización para ello.

Cuadro 10. (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.11.1.6	**Áreas de carga, despacho y acceso público**	PR.AC-2	Establecer las siguientes directrices: a) Establecer que el acceso al área de despacho y de carga desde el exterior de la edificación se debería restringir al personal identificado y autorizado b) definir que el área de despacho y carga se debe diseñar de manera que los suministros se puedan cargar y descargar sin que el personal de despacho tenga acceso a otras partes de la edificación c) establecer que las puertas externas de un área de despacho y carga se aseguran cuando las puertas internas están abiertas d) definir que el material que ingresa se inspecciona y examina para determinar la presencia de explosivos, químicos u otros materiales peligrosos, antes de que se retiren del área de despacho y carga e) establecer que el material que ingresa se registra de acuerdo con los procedimientos de gestión de activos al entrar al sitio f) definir que los despachos entrantes y salientes se están separados físicamente, en donde sea posible g) establecer que el material entrante se inspecciona para determinar evidencia de manipulación durante el viaje. Si se descubre esta manipulación, se debería reportar de inmediato al personal de seguridad.
A.11.2	**Equipos**		

Cuadro 10. . (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.11.2.1	**Ubicación y protección de los equipos**	PR.IP-5	Establecer las siguientes directrices para proteger los equipos: a) Establecer que los equipos están ubicados de manera que se minimice el acceso innecesario a las áreas de trabajo b) definir que las instalaciones de procesamiento de la información que manejan datos sensibles están ubicadas cuidadosamente para reducir el riesgo de que personas no autorizadas puedan ver la información durante su uso c) establecer que las instalaciones de almacenamiento se aseguran para evitar el acceso no autorizado d) definir que los elementos que requieren protección especial se salvaguardan para reducir el nivel general de protección requerida e) establecer los controles para minimizar el riesgo de amenazas físicas y ambientales, (robo, incendio, explosivos, humo, agua (o falla en el suministro de agua, polvo, vibración, efectos químicos, interferencia en el suministro eléctrico, interferencia en las comunicaciones, radiación electromagnética y vandalismo) f) establecer directrices acerca de comer, consumir líquidos y fumar en cercanías de las instalaciones de procesamiento de información g) hacer seguimiento de las condiciones ambientales tales como temperatura y humedad, para determinar las condiciones que puedan afectar adversamente las instalaciones de procesamiento de información h) proteger contra descargas eléctricas atmosféricas se debe aplicar a todas las edificaciones y se deben colocar filtros a todas las líneas de comunicaciones y de potencia entrantes, para la protección contra dichas descargas i) considerar el uso de métodos de protección especial, tales como membranas para teclados, para equipos en ambientes industriales; j) proteger los equipos para procesamiento de información confidencial para minimizar el riesgo de fuga de información debido a emanaciones electromagnéticas.

Cuadro 10. (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.11.2.2	**Servicios de suministro**	ID.BE-4 PR.IP-5	Garantizar el cumplimiento de los servicios de suministro (electricidad, telecomunicaciones, suministro de agua, gas, alcantarillado, ventilación y aire acondicionado) de acuerdo a : a) Cumplir con las especificaciones de los fabricantes de equipos y con los requisitos legales locales; b) evaluar regularmente en cuanto a su capacidad para estar al ritmo del crecimiento e interacciones del negocio con otros servicios de soporte; c) inspeccionar y probar regularmente para asegurar su funcionamiento apropiado; d) si es necesario, contar con alarmas para detectar mal funcionamiento; e) si es necesario, tener múltiples alimentaciones con diverso enrutado físico.
A.11.2.3	**Seguridad en el cableado.**	ID.BE-4 PR.AC-2 PR.IP-5	Establecer las directrices para seguridad del cableado: a) Establecer que las líneas de potencia y de telecomunicaciones que entran a instalaciones de procesamiento de información deben ser subterráneas en donde sea posible, o deben contar con una protección alternativa adecuada b) Establecer que los cables de potencia están separados de los cables de comunicaciones para evitar interferencia c) Definir para sistemas sensibles o críticos los controles adicionales que se deben considerar incluyen: la instalación de Conduit apantallado y recintos o cajas con llave en los puntos de inspección y de terminación el uso de blindaje electromagnético para proteger los cables el inicio de barridos técnicos e inspecciones físicas de dispositivos no autorizados que se conectan a los cables

Cuadro 10. (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.11.2.4	**Mantenimiento de los equipos.**	PR.MA-1 PR.MA-2	Establecer las siguientes directrices para mantenimiento de equipos: a) Mantener los equipos de acuerdo con los intervalos y especificaciones de servicio recomendados por el proveedor b) establecer que solo el personal de mantenimiento autorizado debería llevar a cabo las reparaciones y el servicio a los equipos c) llevar registros de todas las fallas reales o sospechadas, y de todo el mantenimiento preventivo y correctivo d) implementar los controles apropiados cuando el equipo está programado para mantenimiento, teniendo en cuenta si éste lo lleva a cabo el personal en el sitio o personal externo a la organización; en donde sea necesario, la información confidencial se debe borrar del equipo, o el personal de mantenimiento debería retirarse (cleared) lo suficientemente de la información e) cumplir todos los requisitos de mantenimiento impuestos por las políticas de seguros f) establecer que antes de volver a poner el equipo en operación después de mantenimiento, se debería inspeccionar para asegurarse de que no ha sido alterado y que su funcionamiento es adecuado.
A.11.2.5	**Retiro de activos**	PR.MA-1	Establecer las siguientes directrices para el retiro de activos: a) Identificar a los empleados y usuarios de partes externas que tienen autoridad para permitir el retiro de activos del sitio b) establecer los límites de tiempo para el retiro de activos y verificar que se cumplen las devoluciones c) definir cuando sea necesario y apropiado, registrar los activos se retiran del sitio y cuando se hace su devolución d) documentar la identidad, el rol y la filiación de cualquiera que maneje o use activos, y devolver esta documentación con el equipo, la información y el software. Información adicional

Cuadro 10. (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.11.2.6	**Seguridad de equipos y activos fuera de las instalaciones**	ID.AM-4	Establecer las siguientes directrices para proteger los equipos fuera de las instalaciones: a) Establecer que los equipos y medios retirados de las instalaciones no se deben dejar sin vigilancia en lugares públicos b) seguir en todo momento las instrucciones del fabricante para proteger los equipos, (contra exposición a campos electromagnéticos fuertes) c) controlar los lugares fuera de las instalaciones, tales como trabajo en la casa, teletrabajo y sitios temporales se deben determinar mediante una valoración de riesgos y se deben aplicar los controles adecuados según sean apropiados, (gabinetes de archivo con llave, política de escritorio limpio, controles de acceso para computadores y comunicación segura con la oficina) d) establecer que cuando el equipo que se encuentra afuera de las instalaciones es transferido entre diferentes individuos y partes externas, llevar un registro que defina la cadena de custodia para el equipo, que incluya al menos los nombres y las organizaciones de los responsables del equipo.
A.11.2.7	**Disposición segura o reutilización de equipos**	PR.DS-3 PR.IP-6	Establecer las siguientes directrices del proceso de borrado de discos y de encriptación del disco (para evitar la divulgación de la información confidencial cuando se dispone del equipo o se le da un destino diferente, siempre y cuando): a) Establecer que el proceso de encriptación sea suficientemente fuerte y abarque todo el disco (incluido el espacio perdido, archivos temporales de intercambio, etc.) b) Definir que las llaves de encriptación sean lo suficientemente largas para resistir ataques de fuerza bruta c) Establecer que las llaves de encriptación se mantengan confidenciales.

Cuadro 10. (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.11.2.8	**Equipos de usuario desatendido**		Definir el procedimiento de equipos de usuarios desatendidos en donde deben incluir: a) Establecer que se cierren las sesiones activas cuando hayan terminado, a menos que se puedan asegurar mediante un mecanismo de bloqueo apropiado (un protector de pantalla protegido con contraseña) b) establecer que es obligatorio salir de las aplicaciones o servicios de red cuando ya no los necesiten c) asegurar que los computadores o dispositivos móviles contra uso no autorizado mediante el bloqueo de teclas o un control equivalente (acceso con contraseña, cuando no están en uso).
A.11.2.9	**Política de escritorio y pantalla limpios**	PR.PT-2	Establecer las siguientes directrices para escritorio limpio: a) Establecer que la información sensible o crítica del negocio, (sobre papel o en un medio de almacenamiento electrónico), se guarda bajo llave (idealmente, en una caja fuerte o en un gabinete u otro mueble de seguridad) cuando no se requiera, especialmente cuando la oficina esté desocupada. b) Definir un procedimiento para la gestión de equipos desatendidos; los computadores y terminales deben estar fuera del sistema y estar protegidos con un sistema de bloqueo de la pantalla y el teclado, controlado por una contraseña, token o mecanismo similar de autenticación de usuario, y deben estar protegidos por bloqueo de teclas u otros controles, cuando no están en uso c) Evitar el uso no autorizado de fotocopiadoras y otra tecnología de reproducción (escáneres, cámaras digitales) d) Establecer que los medios que contienen información sensible o clasificada se deben retirar de las impresoras inmediatamente.
A.12	**SEGURIDAD DE LAS OPERACIONES**		
A.12.1	**Procedimientos operacionales y responsabilidades**		

Cuadro 10. (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.12.1.1	**Procedimientos de operación documentados**		Establecer los procedimientos de operación con instrucciones operacionales, que incluyen: a) Instalar y configurar sistemas b) establecer el procesamiento y manejo de información, tanto automático como manual; c) Establecer la gestión de las copias de respaldo; d) Definir los requisitos de programación, incluidas las interdependencias con otros sistemas, los tiempos de finalización del primer y último trabajos e) Establecer las instrucciones para manejo de errores u otras condiciones excepcionales que podrían surgir durante la ejecución del trabajo, incluidas las restricciones sobre el uso de sistemas utilitarios f) Definir contactos de apoyo y de una instancia superior, incluidos los contactos de soporte externo, en el caso de dificultades operacionales o técnicas inesperadas g) Establecer las instrucciones sobre manejo de medios y elementos de salida, tales como el uso de papelería especial o la gestión de elementos de salida confidenciales, incluidos procedimientos para la disposición segura de elementos de salida de trabajos fallidos h) Definir los procedimientos de reinicio y recuperación del sistema para uso en el caso de falla del sistema i) Definir la gestión de la información de rastros de auditoría y de información del log del sistema j) Establecer los procedimientos de seguimiento.

Cuadro 10. (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.12.1.2	**Gestión de cambios**	PR.IP-1 PR.IP-3	Definir los procedimientos de control de cambios, que incluyen: a) Identificar y registrar los cambios significativos b) Planificar y puesta a prueba de los cambios c) Valorar los impactos potenciales, incluidos los impactos de estos cambios en la seguridad de la información d) Tener un procedimiento de aprobación formal para los cambios propuestos e) Verificar que se han cumplido los requisitos de seguridad de la información f) Comunicar todos los detalles de los cambios a todas las personas pertinentes g) Tener un procedimiento de apoyo, incluidos procedimientos y responsabilidades para abortar cambios no exitosos y recuperarse de ellos, y eventos no previstos h) Contar con un suministro de un proceso de cambio de emergencia que posibilite la implementación rápida y controlada de los cambios necesarios para resolver un incidente.
A.12.1.3	**Gestión de capacidad**	ID.BE-4	Definir procedimientos para la gestión de la demanda de capacidad, que incluyen: a) Eliminar datos obsoletos (espacio en disco) b) realizar cierre definitivo de aplicaciones, sistemas, bases de datos o ambientes c) optimizar cronogramas y procesos de lotes d) optimizar las consultas de bases de datos o lógicas de las aplicaciones e) realizar una negación o restricción de ancho de banda a servicios ávidos de recursos, si estos no son críticos para el negocio.

Cuadro 10. (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.12.1.4	**Separación de los ambientes de desarrollo, pruebas y operación**	PR.DS-7	Definir los procedimientos para la separación de ambientes, que incluyen: a) Definir y documentar las reglas para la transferencia de software del estatus de desarrollo al de operaciones. b) Establecer que el software de desarrollo y de operaciones debe funcionar en diferentes sistemas o procesadores de computador y en diferentes dominios o directorios c) Definir que los cambios en los sistemas operativos y aplicaciones se deben probar en un entorno de pruebas antes de aplicarlos a los sistemas operacionales d) Definir que solo en circunstancias excepcionales, las pruebas no se deben llevar a cabo en los sistemas operacionales e) establecer que los compiladores, editores y otras herramientas de desarrollo o utilitarios del sistema no debe ser accesibles desde sistemas operacionales cuando no se requiere f) Establecer que los usuarios deben usar diferentes perfiles de usuario para sistemas operacionales y de pruebas, y los menús deben desplegar mensajes de identificación apropiados para reducir el riesgo de error g) Definir que los datos sensibles no se debe copiar en el ambiente del sistema de pruebas, a menos que se suministren controles equivalentes para el sistema de pruebas.
A.12.2	**Protección contra códigos maliciosos**		

Cuadro 10. (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.12.2.1	**Controles contra códigos maliciosos**	PR.DS-6 DE.CM-4 RS. MI-2	Establecer las siguientes directrices: a) Establecer una política formal que prohíba el uso de software no autorizado; b) Implementar controles para evitar o detectar el uso de software no autorizado (listas blancas de aplicaciones); b) Implementar controles para evitar o detectar el uso de sitios web malicioso o que se sospecha que lo son (listas negras); d) Establecer una política formal para proteger contra riesgos asociados con la obtención de archivos y de software ya sea mediante redes externas o cualquier otro medio, indicando qué medidas externas se deben tomar; e) Reducir las vulnerabilidades de las que pueda aprovecharse el software malicioso, (medio de la gestión de la vulnerabilidad técnica) f) Llevar a cabo revisiones regulares del software y del contenido de datos de los sistemas que apoyan los procesos críticos del negocio; se debería investigar formalmente la presencia de archivos no aprobados o de enmiendas no autorizadas g) Instalar y actualizar software de detección y reparación del software malicioso en los computadores y medios como una medida de control, en forma rutinaria; el análisis realizado debería incluir: El análisis de cualquier archivo recibido por la red o por cualquier forma de medio de almacenamiento, para detectar el software malicioso, antes de uso El análisis de los adjuntos y descargas de los correos electrónicos, para determinación del software malicioso antes de uso; este análisis se debería llevar a cabo en diferentes lugares, (los servidores de los correos electrónicos, en los computadores de escritorio) y cuando se

			ingresa a la red de la organización; el análisis de páginas web, para determinar el software malicioso h) definir procedimientos y responsabilidades relacionadas con la protección contra el software malicioso en los sistemas, formación acerca del uso de dichos procedimientos, reporte y recuperación de ataques de software malicioso i) preparar planes de continuidad del negocio apropiados, para la recuperación de ataques de software malicioso, incluidos todos los datos necesarios, copias de respaldo del software y disposiciones para recuperación j) implementar procedimientos para recolectar información en forma regular, (la suscripción a listas de correos o la verificación de sitios web que suministran información acerca de nuevo software malicioso) k) implementar procedimientos para verificar información relacionada con el software malicioso, y asegurarse de que los boletines de advertencia sean exactos e informativos l) alistar entornos en donde se pueden obtener impactos catastróficos.

Cuadro 10. (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.12.3	**Copias de respaldo**		
A.12.3.1	**Respaldo de la información**	PR.DS-4 PR.IP-4	Establecer las siguientes directrices: a) Producir registros exactos y completos de las copias de respaldo, y procedimientos de restauración documentados; b) Establecer la cobertura (copias de respaldo completas o diferenciales) y la frecuencia con que se hagan las copias de respaldo debe reflejar los requisitos del negocio de la organización, los requisitos de la seguridad de la información involucrada, y la criticidad de la información para la operación continua de la organización; c) Definir las copias de respaldo se debe almacenar en un lugar remoto, a una distancia suficiente que permita escapar de cualquier daño que pueda ocurrir en el sitio principal; d) Establecer la información de respaldo y un nivel apropiado de protección física y del entorno, de coherencia con las normas aplicadas en el sitio principal; e) Definir los medios de respaldo se debe poner a prueba regularmente para asegurar que se puede depender de ellos para uso de emergencia en caso necesario; esto se debería combinar con una prueba de los procedimientos de restauración, y se debe verificar contra el tiempo de restauración requerido. f) Definir las situaciones en las que la confidencialidad tiene importancia, las copias de respaldo deben estar protegidas por medio de encriptación.
A.12.4	**Registro y seguimiento**		

Cuadro 10. (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.12.4.1	**Registro de eventos**	PR.PT-1 DE.CM-3 RS.AN-1	Establecer el registro de eventos en donde deben incluir: a) Identificación de los usuarios b) Establecer las actividades del sistema c) Definir las fechas, horas y detalles de los eventos clave, (entrada y salida) d) Identificar el dispositivo o ubicación, si es posible, e identificador del sistema e) Tener registros de intentos de acceso al sistema exitosos y rechazados e) Definir registros de datos exitosos y rechazados y otros intentos de acceso a recursos; g) Establecer los cambios a la configuración del sistema h) definir el uso de privilegios i) Establecer el uso de utilitarios y aplicaciones del sistema j) Definir los archivos a los que se tuvo acceso, y el tipo de acceso k) Establecer las direcciones y protocolos de red; l) Definir las alarmas accionadas por el sistema de control de acceso m) Activar y desactivar los sistemas de protección, tales como sistemas antivirus y sistemas de detección de intrusión n) Registrar las transacciones ejecutadas por los usuarios en las aplicaciones.
A.12.4.2	**Protección de la información de registro**	PR.PT-1	Establecer los procedimientos y controles dirigidos a proteger contra cambios no autorizados de la información del registro y contra problemas con la instalación de registro, que incluya: a) verificar todas las alteraciones a los tipos de mensaje que se registran b) establecer los archivos log que son editados o eliminados c) verificar cuando se excede la capacidad de almacenamiento del medio de archivo log, lo que da como resultado falla en el registro de eventos, o sobre escritura de eventos pasados registrados.

Cuadro 10. (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.12.4.3	**Registros del administrador y del operador**	PR.PT-1 RS.AN-1	Garantizar los registros de las actividades del administrador y del operador del sistema, los registros se deben proteger y revisar con regularidad.
A.12.4.4	**Sincronización de relojes**	PR.PT-1	Establecer la sincronización con una única fuente de referencia de tiempo, Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deberían sincronizar con una única fuente de referencia de tiempo.

Cuadro 10. . (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.12.5	**Control de software operacional**		
A.12.5.1	**Instalación de software en sistemas operativos**	PR.DS-6 PR.IP-1 PR.IP-3 DE.CM-5	Establecer las siguientes directrices para control de software operacional: a) Actualizar el software operacional, aplicaciones y bibliotecas de programas solo la debe llevar a cabo administradores entrenados, con autorización apropiada de la dirección b) Definir que los sistemas operacionales sólo debe contener códigos ejecutables aprobados, no el código de desarrollo o compiladores c) Establecer que las aplicaciones y el software del sistema operativo solo se debe implementar después de pruebas extensas y exitosas; los ensayos deben abarcar la usabilidad, la seguridad, los efectos sobre otros sistemas y la facilidad de uso, y se debe llevar a cabo en sistemas separados se debe asegurar que todas las bibliotecas de fuentes de programas correspondientes hayan sido actualizadas d) Usar un sistema de control de la configuración para mantener el control de todo el software implementado, al igual que la documentación del sistema e) establecer una estrategia de retroceso (rollback) antes de implementar los cambios f) Mantener un log de auditoría de todas las actualizaciones de las bibliotecas de programas operacionales g) Definir las versiones anteriores del software de aplicación se deben conservar como una medida de contingencia h) Establecer que las versiones de software anteriores se deben llevar al archivo permanente, junto con toda la información y parámetros, procedimientos, detalles de configuración y software de soporte anteriores, en tanto los datos permanezcan en el archivo permanente.

Cuadro 10. (continuidad)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.12.6	**Gestión de la vulnerabilidad técnica**		
A.12.6.1	**Gestión de las vulnerabilidades técnicas**	ID.RA-1 ID.RA-5 PR.IP-12 DE.CM-8 RS.MI-3	Establecer las siguientes directrices para vulnerabilidades técnicas: a) Definir y establecer los roles y responsabilidades asociados con la gestión de la vulnerabilidad técnica, incluido el seguimiento de la vulnerabilidad, la valoración de riesgos de vulnerabilidad, la colocación de parches, el seguimiento de activos y cualquier responsabilidad de coordinación requerida b) definir los recursos de información que se usarán para identificar las vulnerabilidades técnicas pertinentes y para mantener la toma de conciencia acerca de ellos se debe identificar para el software y otra tecnología c) una línea de tiempo para reaccionar a las notificaciones de vulnerabilidades técnicas pertinentes potencialmente d) establecer que una vez que se haya identificado una vulnerabilidad técnica potencial, la organización debería identificar los riesgos asociados y las acciones por tomar; esta acción puede involucrar la colocación de parches de sistemas vulnerables o la aplicación de otros controles; Si no es posible colocar controles se deben documentar en los riesgos de acuerdo a su probabilidad e impacto y colocarlo como riesgo aceptado. e) definir dependiendo de la urgencia con la que se necesite tratar una vulnerabilidad técnica, la acción tomada se debería llevar a cabo de acuerdo con los controles relacionados con la gestión de cambios, o siguiendo los procedimientos de respuesta a incidentes de seguridad de la información f) establecer, si está disponible un parche de una fuente legítima, se debe valorar los riesgos asociados con la instalación del parche (los riesgos que acarrea la vulnerabilidad se debe comparar con el riesgo de instalar el

			parche) g) establecer que los parches se deben probar y evaluar antes de su instalación, para asegurarse de que son eficaces y no producen efectos secundarios que no se puedan tolerar; si no hay parches disponibles, se debe considerar otros controles como: dejar de operar los servicios o capacidades relacionados con la vulnerabilidad adaptar o adicionar controles de acceso, (cortafuegos, en los límites de la red) incrementar el seguimiento para detectar ataques reales tomar conciencia sobre la vulnerabilidad h) llevar un log de auditoría para todos los procedimientos realizados i) hacer seguimiento y evaluación regulares del proceso de gestión de vulnerabilidad técnica, con el fin de asegurar su eficacia y eficiencia j) abordar primero los sistemas que están en alto riesgo k) establecer un proceso de gestión eficaz de la vulnerabilidad técnica alineada con las actividades de gestión de incidentes para comunicar los datos sobre vulnerabilidades a la función de respuesta a incidentes y suministrar los procedimientos técnicos para realizarse si llegara a ocurrir un incidente l) definir un procedimiento para hacer frente a una situación en la que se ha identificado una vulnerabilidad, pero no hay una contramedida adecuada. En esta situación, la organización debería evaluar los riesgos relacionados con la vulnerabilidad conocida y definir las acciones de detección y correctivas apropiadas.
A.12.6.2	**Restricciones sobre la instalación de software**	PR.IP-1 PR.IP-3	Establecer las restricciones y las reglas para la instalación de software por parte de los usuarios.
A.12.7	**Consideraciones sobre auditorias de sistemas de información**		

Cuadro 10. (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.12.7.1	**Controles de auditorías de sistemas de información**		Establecer las siguientes directrices para las auditorias de sistemas de información: a) Establecer los requisitos de auditoría para acceso a sistemas y a datos se debe acordar con la dirección apropiada b) definir el alcance de las pruebas técnicas de auditoría se debe acordar y controlar c) establecer las pruebas de auditoría se debe limitar a acceso a software y datos únicamente para lectura d) definir el acceso diferente al de solo lectura solamente se debe prever para copias aisladas de los archivos del sistema, que se deben borrar una vez que la auditoría haya finalizado, o se debe proporcionar información apropiada si hay obligación de mantener estos archivos bajo los requisitos de documentación de auditoría e) definir los requisitos para procesos especiales y adicionales se debe identificar y acordar; f) establecer las pruebas de auditoría que puedan afectar la disponibilidad del sistema se deben realizar fuera de horas laborales g) hacer seguimiento de todos los accesos y logged para producir un rastro de referencia.
A.13	**SEGURIDAD DE LAS COMUNICACIONES**		
A.13.1	**Gestión de la seguridad de las redes**		

Cuadro 10. . (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.13.1.1	**Controles de redes**	PR.AC-3 PR.AC-5 PR.DS-2 PR.PT-4	Establecer las siguientes directrices para la gestión de seguridad de redes: a) Establecer las responsabilidades y procedimientos para la gestión de equipos de redes b) Definir la responsabilidad operacional por las redes se debería separar de las operaciones informáticas, en donde sea apropiado c) Establecer controles especiales para salvaguardar la confidencialidad e integridad de los datos que pasan sobre redes públicas o sobre redes inalámbricas, y para proteger los sistemas y aplicaciones conectados d) Gestionar el acceso remoto d) Aplicar logging y seguimiento adecuados para posibilitar el registro y detección de acciones que pueden afectar, o son pertinentes a la seguridad de la información e) Definir las actividades de gestión a coordinar estrechamente tanto para optimizar el servicio de la organización, como para asegurar que los controles se apliquen en forma coherente a través de la infraestructura de procesamiento de información f) Establecer los sistemas en la red que se autenticar g) Restringir la conexión de los sistemas a la red.
A.13.1.2	**Seguridad de los servicios de red**		Establecer las siguientes directrices para la seguridad de los servicios de red: a) Establecer la tecnología aplicada a la seguridad de servicios de red, tales como autenticación, encriptación y controles de conexión de red b) Definir los parámetros técnicos requeridos para la conexión segura con los servicios de red de acuerdo con las reglas de conexión de seguridad y de red c) Establecer los procedimientos para el uso de servicios de red para restringir el acceso a los servicios o aplicaciones de red, cuando sea necesario.

Cuadro 10. . (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.13.1.3	**Separación en las redes**	PR.AC-5 PR.DS-5	Para proteger la integridad de las redes es necesario incorporar la segregación de la red en donde se requiera.
A.13.2	**Transferencia de información**		
A.13.2.1	**Políticas y procedimientos de transferencia de información**	ID.AM-3 PR.AC-5 PR.AC-3 PR.DS-2 PR.DS-5 PR.PT-4	Establecer las siguientes directrices: a) Definir los procedimientos diseñados para proteger la información transferida contra interceptación, copiado, modificación, enrutado y destrucción b) Definir los procedimientos para la detección de software malicioso y protección contra éste, que puede ser transmitido mediante el uso de comunicaciones electrónicas c) Definir los procedimientos para proteger información electrónica sensible comunicada que están como adjuntos d) Establecer la política o directrices que presentan el uso aceptable de las instalaciones de comunicación e) Definir las responsabilidades del personal, las partes externas y cualquier otro usuario no comprometen a la organización, (por difamación, acoso, suplantación, envío de cadenas, compras no autorizadas, etc.) f) Establecer el uso de técnicas criptográficas, (proteger la confidencialidad, la integridad y la autenticidad de la información). g) Establecer las directrices sobre retención y disposición para toda la correspondencia del negocio, incluidos mensajes, de acuerdo con la legislación y reglamentaciones locales y nacionales h) Definir los controles y restricciones asociadas con las instalaciones de comunicación, (el reenvío automático de correo electrónico a direcciones de correo externas) i) Brindar asesoría al personal para que tome las precauciones apropiadas acerca de no revelar información confidencial

			j) No dejar mensajes que contengan información confidencial, en las máquinas contestadoras, ya que éstos pueden ser escuchados por personas no autorizadas, almacenados en sistemas comunales o almacenados incorrectamente como resultado de una marcación incorrecta k) Brindar asesoría al personal acerca de los problemas de usar máquinas o servicios de fax, a saber: acceso no autorizado a almacenes de mensajes built-in para recuperar mensajes, programar las máquinas en forma deliberada o accidental para enviar mensajes a números específicos, enviar documentos y mensajes a un número equivocado, ya sea por marcación errada o por marcar un número almacenado equivocado.

Cuadro 10. (Continuara)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.13.2.2	**Acuerdos sobre transferencia de información**		Establecer las siguientes directrices para transferencia segura de la información: a) Establecer las responsabilidades de la dirección para controlar y notificar la transmisión, despacho y recibo b) Definir los procedimientos para asegurar trazabilidad y no repudio c) Definir los estándares técnicos mínimos para empaquetado y transmisión d) tener certificados de depósito de títulos en garantía e) Establecer los estándares de identificación de mensajería f) Definir las responsabilidades y obligaciones en el caso de incidentes de seguridad de la información, tales como pérdidas de datos g) Establecer el uso de un sistema de etiquetado acordado para información sensible o crítica, que asegure que el significado de la etiqueta se entiende de inmediato, y que la información está protegida apropiadamente h) Definir las normas técnicas para registro y lectura de información y software i) Cualquier control especial que se requiera para proteger elementos críticos, tales como criptografía; j) Mantener una cadena de custodia para la información mientras está en tránsito k) Definir los niveles aceptables de control de acceso.

Cuadro 10. (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.13.2.3	**Mensajería Electrónica**	PR.DS-2 PR.DS-5	Establecer las siguientes directrices para mensajería electrónica: a) Definir la protección de mensajes contra acceso no autorizado, modificación o denegación del servicio proporcionales al esquema de clasificación adoptado por la organización b) Asegurar el direccionamiento y transporte correctos del mensaje c) Establecer la confiabilidad y disponibilidad del servicio d) Definir las consideraciones legales, (los requisitos para firmas electrónicas e) Establecer la obtención de aprobación antes de usar servicios públicos externos como mensajería instantánea, redes sociales o intercambio de información) f) Definir niveles más fuertes de autenticación para control del acceso desde redes accesibles públicamente.

Cuadro 10. (continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.13.2.4	**Acuerdos de confidencialidad o de no divulgación**	PR.DS-5	Establecer las siguientes directrices para acuerdos de confidencialidad: a) Definir la información que se va a proteger (información confidencial) b) Determinar la duración esperada de un acuerdo, incluidos los casos en los que podría ser necesario mantener la confidencialidad indefinidamente c) Establecer las acciones requeridas cuando termina el acuerdo d) Definir las responsabilidades y acciones de los firmantes para evitar la divulgación no autorizada de información e) Definir la propiedad de la información, los secretos comerciales y la propiedad intelectual, y cómo esto se relaciona con la protección de información confidencial f) Definir el uso permitido de información confidencial y los derechos del firmante para usar la información g) Establecer el derecho a actividades de auditoría y de seguimiento que involucran información confidencial h) Definir el proceso de notificación y reporte de divulgación no autorizada o fuga de información confidencial i) Definir los plazos para que la información sea devuelta o destruida al cesar el acuerdo j) Establecer las acciones que se espera tomar en caso de violación del acuerdo.

Cuadro 10. . (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.14	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**		
A.14.1	**Requisitos de seguridad de los sistemas de información**		
A.14.1.1	**Análisis y especificación de requisitos de seguridad de la información**	PR.IP-2	Establecer las siguientes directrices para análisis y especificaciones de requisitos de seguridad de la información: a) Establecer el nivel de confianza requerido con relación a la identificación declarada de los usuarios, para obtener los requisitos de autenticación de usuario. b) Definir los procesos de suministro de acceso y de autorización para usuarios del negocio, al igual que para usuarios privilegiados o técnicos c) Informar a los usuarios y operadores sobre sus deberes y responsabilidades d) Definir las necesidades de protección de activos involucrados, en particular acerca de disponibilidad, confidencialidad, integridad e) Definir los requisitos obtenidos de los procesos del negocio, tales como los requisitos de ingreso y seguimiento, y de no repudio f) Establecer los requisitos exigidos por otros controles de seguridad, (interfaces con el ingreso o seguimiento, o los sistemas de detección de fuga de datos).

Cuadro 10. . (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.14.1.2	**Seguridad de servicios de las aplicaciones en redes públicas**	PR.DS-2 PR.DS-5 PR.DS-6	Establecer las siguientes directrices para la seguridad de servicios de las aplicaciones en redes públicas: a) Definir el nivel de confianza que cada parte requiere con relación a la identidad declarada por la otra parte, (por medio de autenticación) b) Establecer los procesos de autorización asociados con quien puede aprobar el contenido o expedir o firmar documentos transaccionales clave c) Asegurar que los socios de comunicación estén completamente informados de sus autorizaciones para suministro o uso del servicio d) Determinar y cumplir los requisitos para confidencialidad, integridad, prueba de despacho y recibo de documentos clave y el no repudio de los contratos, (asociados con procesos de ofertas y contratos) e) Definir el nivel de confianza requerido en la integridad de los documentos clave f) Establecer los requisitos de protección de cualquier información confidencial g) Definir la confidencialidad e integridad de cualquier transacción de pedidos, información de pagos, detalles de la dirección de entrega y confirmación de recibos; h) Definir el grado de verificación apropiado de la información de pago suministrada por un cliente i) Seleccionar la forma de arreglo de pago más apropiado para protegerse contra fraude; j) Definir el nivel de protección requerido para mantener la confidencialidad e integridad de la información del pedido k) Evitar la pérdida o duplicación de información de la transacción l) definir la responsabilidad civil asociada con cualquier transacción fraudulenta m) Establecer los requisitos de seguros. n) Usar mecanismos de chequeo de la integridad para verificar la integridad del software, firmware, e información

Cuadro 10. (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.14.1.3	**Protección de transacciones de los servicios de las aplicaciones.**	PR.DS-2 PR.DS-5 PR.DS-6	Establecer las siguientes directrices protección de transacciones de los servicios de las aplicaciones: a) Definir el uso de firmas electrónicas por cada una de las partes involucradas en la transacción b) Establecer todos los aspectos de la transacción, es decir, asegurar que: 1) definir la información de autenticación secreta de usuario, de todas las partes, se valide y verifique 2) Definir a transacción permanezca confidencial 3) mantener la privacidad asociada con todas las partes involucradas c) Definir la trayectoria de las comunicaciones entre todas las partes involucradas esté encriptada d) Definir los protocolos usados para comunicarse entre todas las partes involucradas estén asegurados e) Asegurar que el almacenamiento de los detalles de la transacción esté afuera de cualquier entorno accesible públicamente, (en una plataforma de almacenamiento existente en la intranet de la organización, y no retenido ni expuesto en un medio de almacenamiento accesible directamente desde Internet) f) Utilizar una autoridad confiable (para los propósitos de emitir y mantener firmas digitales o certificados digitales), la seguridad está integrada e incluida en todo el proceso de gestión de certificados/firmas de un extremo a otro.

Cuadro 10. .(Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.14.2	**Seguridad en los procesos de Desarrollo y de Soporte**		
A.14.2.1	**Política de desarrollo seguro**	PR.IP-2	Establecer las siguientes directrices política de desarrollo seguro: a) Definir la seguridad del ambiente de desarrollo b) Orientar la seguridad en el ciclo de vida de desarrollo del software: 1) Definir la seguridad en la metodología de desarrollo de software 2) Establecer las directrices de codificación seguras para cada lenguaje de programación usado c) Definir los requisitos de seguridad en la fase diseño d) Definir los puntos de chequeo de seguridad dentro de los hitos del proyecto e) establecer los depósitos seguros f) Definir la seguridad en el control de la versión g) Establecer el conocimiento requerido sobre seguridad de la aplicación h) Definir la capacidad de los desarrolladores para evitar, encontrar y resolver las vulnerabilidades.

Cuadro 10. .(Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.14.2.2	**Procedimientos de control de cambios en sistemas**	PR.IP-1 PR.IP-3	Establecer las siguientes directrices procedimientos control de cambio en sistemas: a) Llevar un registro de los niveles de autorización acordados b) asegurar que los cambios se presenten a los usuarios autorizados c) Revisar los controles y procedimientos de integridad para asegurar que no se vean comprometidos por los cambios d) Identificar todo el software, información, entidades de bases de datos y hardware que requieren corrección e) Identificar y verificar el código crítico de seguridad para minimizar la posibilidad de debilidades de seguridad conocidas f) Obtener aprobación formal para propuestas detalladas antes de que el trabajo comience g) Revisar antes de la implementación, asegurar que los usuarios autorizados aceptan los cambios h) Asegurar que el conjunto de documentación del sistema está actualizado al completar cada cambio, y que la documentación antigua se lleva al archivo permanente, o se dispone de ella i) Mantener un control de versiones para todas las actualizaciones de software j) Mantener un rastro de auditoría de todas las solicitudes de cambio k) Asegurar que la documentación de operación y los procedimientos de los usuarios experimenten los cambios que les permitan seguir siendo apropiados l) Asegurar que la implementación de los cambios ocurre en el momento correcto y no afecta los procesos de negocio involucrados.

Cuadro 10. . (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.14.2.3	**Revisión técnica de las aplicaciones después de cambios en la plataforma de operación**	PR.IP-1	Establecer las directrices revisión técnica de las aplicaciones después de cambios en la plataforma de operación: a) Revisar los procedimientos de integridad y control de aplicaciones para asegurar que no estén comprometidos debido a los cambios en las plataformas de operaciones b) Asegurar que la notificación de los cambios en la plataforma operativa se hace a tiempo para permitir las pruebas y revisiones apropiadas antes de la implementación c) Asegurar que se hacen cambios apropiados en los planes de continuidad del negocio.
A.14.2.4	**Restricciones en los cambios a los paquetes de software**	PR.IP-1	Establecer las siguientes directrices restricciones en los cambios a los paquetes de software: a) Definir el riesgo de que los procesos de integridad y los controles incluidos se vean comprometidos b) Obtener el consentimiento del vendedor c) Obtener del vendedor los cambios requeridos, a medida que se actualiza el programa estándar d) Evaluar el impacto, si la organización llega a ser responsable del mantenimiento futuro del software como resultado de los cambios e) Definir la compatibilidad con otro software en uso.
A.14.2.5	**Principio de Construcción de los Sistemas Seguros.**	PR.IP-2	Solicitar la documentación y los principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.

Cuadro 10. . (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.14.2.6	**Ambiente de desarrollo seguro**		Establecer las siguientes directrices para ambiente de desarrollo seguro: a) Carácter sensible de los datos que el sistema va a procesar, almacenar y transmitir b) Definir los requisitos externos e internos aplicables, (reglamentaciones o políticas) c) Definir los controles de seguridad ya implementados por la organización, que brindan soportar al desarrollo del sistema d) Establecer la confiabilidad del personal que trabaja en el ambiente e) Definir el grado de contratación externa asociado con el desarrollo del sistema f) definir la necesidad de separación entre diferentes ambientes de desarrollo g) Definir el control de acceso al ambiente de desarrollo h) Establecer el seguimiento de los cambios en el ambiente y en los códigos almacenados ahí i) Definir las copias de respaldo se almacenan en lugares seguros fuera del sitio j) Definir el control sobre el movimiento de datos desde y hacia el ambiente.

Cuadro 10. . (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.14.2.7	**Desarrollo contratado externamente**	DE.CM-6	Establecer las siguientes directrices desarrollo contratado externamente: a) Definir los acuerdos de licenciamiento, propiedad de los códigos y derechos de propiedad intelectual relacionados con el contenido contratado externamente b) Establecer los requisitos contractuales para prácticas seguras de diseño, codificación y pruebas c) Definir el suministro del modelo de amenaza aprobado, al desarrollador externo d) realizar los ensayos de aceptación para determinar la calidad y exactitud de los entregables e) Definir la evidencia de que se usaron umbrales de seguridad para establecer niveles mínimos aceptables de calidad de la seguridad y de la privacidad f) Definir la evidencia de que se han hecho pruebas suficientes para proteger contra contenido malicioso intencional y no intencional en el momento de la entrega g) Definir la evidencia de que se han hecho pruebas suficientes para proteger contra la presencia de vulnerabilidades conocidas h) Definir los certificados de depósito de títulos en garantía (el código fuente ya no está disponible) i) Establecer el derecho contractual con relación a procesos y controles de desarrollo de auditorías j) Documentar eficaz del ambiente de construcción usado para crear entregables k) Establecer que la organización es responsable de la conformidad con las leyes aplicables y con la verificación de la eficiencia del control.

Cuadro 10. . (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.14.2.8	**Pruebas de seguridad de sistemas**	DE.DP-3	Realizar pruebas de seguridad debidamente documentadas. Tal igual que los procesos de detección de incidentes sean probados periódicamente.
A.14.2.9	**Prueba de aceptación de sistemas**		Realizar y documentar las pruebas de aceptación de sistemas, para los sistemas de información nuevos, actualizaciones y nuevas versiones, es necesario establecer programas de prueba para aceptación y criterios de aceptación relacionados
A.14.3	**Datos de prueba**		
A.14.3.1	**Protección de datos de prueba**		Establecer las siguientes directrices para protección de datos de prueba: a) Establecer los procedimientos de control de acceso, que se aplican a los sistemas de aplicación operacionales, se debe aplicar también a los sistemas de aplicación de pruebas b) Tener una autorización separada cada vez que se copia información operacional a un ambiente de pruebas c) Definir que la información operacional se debe borrar del ambiente de pruebas inmediatamente después de finalizar las pruebas d) Establecer que el copiado y uso de la información operacional se debe logged para suministrar un rastro de auditoría.

Cuadro 10. (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.15	**RELACIONES CON LOS PROVEEDORES**		
A.15.1	**Seguridad de la información en las relaciones con los proveedores.**		1)Definir la política de seguridad de la información para las relaciones con los proveedores, que indique los requisitos de SI para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización, esta política debe reflejarse en los acuerdos con los proveedores que deben estar documentados. 2) Establecer con los proveedores que cuentan con acceso a los activos de información (no necesariamente son proveedores de tecnología de la información, por ejemplo pueden ser proveedores que tengan por ejemplo un proceso de nómina en outsourcing), se hayan suscrito acuerdos (ANS) formales donde se establezcan y acuerden todos los requisitos de seguridad de la información pertinentes. 3)Establecer con los proveedores si se tiene en cuenta los riesgos de SI asociados a la cadena de suministro, por ejemplo para los proveedores en la nube es muy común que se apoyen en otros proveedores para proporcionar las instalaciones y se deben manejar los riesgos asociados a este tercero con el cual la entidad no tiene una relación comercial directa. Solicite que le indiquen como identifican para cada proveedor su cadena de suministro y obtenga evidencia de este hecho.
A.15.2	**Gestión de la prestación de servicios de proveedores**		1) Realizar el seguimiento, revisar y auditar con regularidad de acuerdo a la política la prestación de servicios de los proveedores y el cumplimiento de los compromisos respecto a la seguridad de la información. 2) Gestionar y documentar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes , teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, los incidentes de seguridad de la información y la revaloración de los riesgos.

Cuadro 10. , (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.16	**GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**		
A.16.1	**Gestión de incidentes y mejoras en la seguridad de la información**		
A.16.1.1	**Responsabilidades y procedimientos**	PR.IP-9 DE.AE-2 RS.CO-1	Establecer las directrices frente a responsabilidades y procedimientos: a) Establecer las responsabilidades de gestión, para asegurar que los siguientes procedimientos se desarrollan y comunican adecuadamente dentro de la organización: 1) Los procedimientos para la planificación y preparación de respuesta a incidentes 2) Los procedimientos para seguimiento, detección, análisis y reporte de eventos e incidentes de seguridad de la información 3) Los procedimientos para logging las actividades de gestión de incidentes 4) Los procedimientos para el manejo de evidencia forense 5) Los procedimientos para la valoración y toma de decisiones sobre eventos de seguridad de la información y la valoración de debilidades de seguridad de la información 6) Los procedimientos para respuesta, incluyendo aquellos para llevar el asunto a una instancia superior, recuperación controlada de un incidente y comunicación a personas u organizaciones internas y externas b) Establecer los procedimientos para asegurar que: 1) El personal competente maneje las cuestiones relacionadas con incidentes de seguridad de la información dentro de la organización 2) Se implemente un punto de contacto para la detección y reporte de incidentes de seguridad 3) Se mantengan contactos apropiados con las autoridades, grupos de interés o foros externos que manejen las cuestiones relacionadas con incidentes de seguridad de la información

			c) Definir el reporte de procedimientos debería incluir: 1) La preparación de formatos de reporte de eventos de seguridad de la información para apoyar la acción de reporte y ayudar a la persona que reporta a recordar todas las acciones necesarias en caso de un evento de seguridad de la información 2) El procedimiento que se va a seguir en el caso de un evento de seguridad de la información, (tomar nota inmediatamente de todos los detalles, tales como el tipo de no conformidad o violación, mal funcionamiento, mensajes en la pantalla y reporte inmediato al punto de contacto y realizar solamente acciones coordinadas) 3) Referencia a un proceso disciplinario formal establecido para ocuparse de los empleados que cometen violaciones a la seguridad 4) Los procesos de retroalimentación adecuados para asegurar que las personas que reportan eventos de seguridad de la información sean notificadas de los resultados después de que la cuestión haya sido tratada y cerrada.

Cuadro 10. (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.16.1.2	**Reporte de eventos de seguridad de la información**	DE.DP-4	Establecer las siguientes directrices frente al reporte de eventos de seguridad de la información: a) Establecer un control de seguridad ineficaz b) Definir la violación de la integridad, confidencialidad o expectativas de disponibilidad de la información c) Definir los errores humanos d) definir las no conformidades con políticas o directrices e) Definir las violaciones de acuerdos de seguridad física f) Establecer los cambios no controlados en el sistema. g) Definir mal funcionamiento en el software o hardware h) definir violaciones de acceso.
A.16.1.3	**Reporte de debilidades de seguridad de la información**	RS.CO-2	Establecer la forma y los medios mediante los cuales se reportan las debilidades de seguridad mediante los criterios establecidos.
A.16.1.4	**Evaluación de eventos de seguridad de la información y decisiones sobre ellos**	DE.AE-2 RS.AN-4	Realizar el análisis de los eventos de SI detectados, con el propósito de determinar si constituyen un incidente de seguridad de la información de esta manera entender los objetivos del ataque y sus métodos. Categorizar los incidentes y contar con planes de respuesta para cada categoría.

Cuadro 10. . (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.16.1.5	**Respuesta a incidentes de seguridad de la información**	RS.RP-1 RS.AN-1 RS. MI-2 RC.RP-1 RC.RP-1	Establecer las siguientes directrices para respuesta a incidentes de seguridad de la información: a) Los incidentes son contenidos y la probabilidad de que vuelvan a ocurrir mitigada. b) Se debe contar con un plan de recuperación de incidentes durante o después del mismo. b) recolectar evidencia lo más pronto posible después de que ocurra el incidente c) llevar a cabo análisis forense de seguridad de la información, según se requiera d) llevar el asunto a una instancia superior, según se requiera e) asegurar que todas las actividades de respuesta involucradas se registren adecuadamente para análisis posterior f) comunicar la existencia del incidente de seguridad de la información o de cualquier detalle pertinente a él, al personal interno o externo a las organizaciones que necesitan saberlo g) tratar las debilidades de seguridad de información que se encontraron que causan o contribuyen al incidente g) establecer que una vez que el incidente se haya tratado lo suficiente, cerrarlo formalmente y hacer un registro de esto.
A.16.1.6	**Aprendizaje obtenido de los incidentes de seguridad de la información**	DE.DP-5 RS.AN-2 RS.IM-1	Documentar y entender cuál fue el impacto del incidente. Las lecciones aprendidas deben ser usadas para actualizar los planes de respuesta a los incidentes de SI.

Cuadro 10. . (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.16.1.7	**Recolección de evidencia**	RS.AN-3	Establecer las siguientes directrices para recolección de evidencia: a) Definir la cadena de custodia b) Establecer la seguridad de la evidencia c) Definir la seguridad del personal d) Definir los roles y responsabilidades del personal involucrado e) Establecer la competencia del personal f) Realizar la documentación g) Definir las sesiones informativas.

Cuadro 10. . (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.17	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO**		
A.17.1	**Continuidad de Seguridad de la información**		
A.17.1.1	**Planificación de la continuidad de la seguridad de la información**	ID. BE-5 PR. IP-9	Indagar si la Entidad cuenta con un BCP (Bussines Continuity Plan) o DRP (Disaster Recovery Plan). Determine si aplica para procesos críticos solamente o se han incluido otros procesos o por lo menos se ha reconocido la necesidad de ampliarlo a otros procesos (para determinar el nivel de madurez) Evalúe si se ha incluido en estos planes y procedimientos los requisitos de seguridad de la información. Tenga en cuenta que en ausencia de una planificación formal de continuidad de negocio y recuperación de desastres, la dirección de seguridad de la información debería suponer que los requisitos de seguridad de la información siguen siendo los mismos en situaciones adversas, en comparación con las condiciones operacionales normales. Como alternativa, una organización puede llevar a cabo un análisis de impacto en el negocio de los aspectos de seguridad de la información, para determinar los requisitos de seguridad de la información aplicables a situaciones adversas. De acuerdo con la NIST también se deben tener planes de respuesta a incidentes y recuperación de incidentes. Tenga en cuenta para la calificación: 1) Si existen planes de continuidad del negocio que contemplen los procesos críticos de la Entidad que garanticen la continuidad de estos. Se documentan tan y protegen adecuadamente los planes de continuidad del negocio de la Entidad, este de estar documentado y firmado, por la alta Dirección, están en 40. 2) Si se reconoce la importancia de ampliar los planes de continuidad de del negocio a otros procesos, pero aún no se pueden incluir ni trabajar con ellos, están en 60.

Cuadro 10. (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.17.1.2	**Implementación de la continuidad de la seguridad de la información**	ID.BE-5 PR.IP-4 PR.IP-9 PR.IP-9	Verifique si la entidad cuenta con a) Una estructura organizacional adecuada para prepararse, mitigar y responder a un evento contingente, usando personal con la autoridad, experiencia y competencia necesarias. b) Personal formalmente asignado de respuesta a incidentes con la responsabilidad, autoridad y competencia necesarias para manejar un incidente y mantener la seguridad de la información. c) Planes aprobados, procedimientos de respuesta y recuperación documentados, en los que se especifique en detalle como la organización gestionará un evento contingente y mantendrá su seguridad de la información en un límite predeterminado, con base en los objetivos de continuidad de seguridad de la información aprobados por la dirección. Revise si los controles de seguridad de la información que se han implementado continúan operando durante un evento contingente. Si los controles de seguridad no están en capacidad de seguir brindando seguridad a la información, se la Entidad debe establecer, implementar y mantener otros controles para mantener un nivel aceptable de seguridad de la información.

Cuadro 10. . (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.17.1.3	**Verificación, revisión y evaluación de la continuidad de la seguridad de la información**	PR.IP-4 PR.IP-10	Indague y solicite evidencias de la realización de pruebas de la funcionalidad de los procesos, procedimientos y controles de continuidad de la seguridad de la información, para asegurar que son coherentes con los objetivos de continuidad de la seguridad de la información Tenga en cuenta que la verificación de los controles de continuidad de la seguridad de la información es diferente de las pruebas y verificación generales de seguridad de la información. Si es posible, es preferible integrar la verificación de los controles de continuidad de negocio de seguridad de la información con las pruebas de recuperación de desastres y de continuidad de negocio de la organización.
A.17.2	**Redundancias**		
A.17.2.1	**Disponibilidad de instalaciones de procesamiento de información**	ID.BE-5	Contar con arquitecturas redundantes, ya sea un centro de cómputo principal y otro alterno o componentes redundantes en el único centro de cómputo. el cual debe ser definido de acuerdo con las necesidades de los procesos para seleccionar que elementos deben ser redundantes. Igualmente documentar las pruebas aplicadas para asegurar que un componente redundante funciona de la forma prevista durante una emergencia o falla.
A.18	**CUMPLIMIENTO**		
A.18.1	**Cumplimiento de requisitos legales y contractuales**	**ID.GV-3**	Los requerimientos legales y regulatorios respecto de la ciberseguridad, incluyendo la privacidad y las libertades y obligaciones civiles, son entendidos y gestionados.

Cuadro 10. . (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.18.1.1	**Identificación de la legislación aplicable.**		Documentar la relación de requisitos legales, reglamentarios, estatutarios, que le aplican a la Entidad (Normograma). Se debe definir el responsable de identificarlos y los responsables para su cumplimiento.
A.18.1.2	**Derechos propiedad intelectual (DPI)**		1) Definir los procedimientos para el cumplimiento de los requisitos y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados. 2)Definir una política publicada sobre el cumplimiento de derechos de propiedad intelectual que defina el uso legal del software y de productos informáticos. Esta política debe estar orientada no solo al software, sino también a documentos gráficos, libros, etc. 3) Establecer el control para que no se instale software ilegal. 4) Realizar un inventario de software instalado y compararlo con el número de licencias adquiridas para asegurar que no se incumplen los derechos de propiedad intelectual.
A.18.1.3	**Protección de registros**	PR.IP-4	Establecer tablas de retención documental que especifiquen los registros y el periodo por el cual se deberían retener, además del almacenamiento, manejo y destrucción. Posibles tipos de registros pueden ser registros contables, registros de bases de datos, logs de transacciones, logs de auditoría y procedimientos operacionales, los medios de almacenamiento permitidos pueden ser papel, microfichas, medios magnéticos, medios ópticos etc.

Cuadro 10. . (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.18.1.4	**Privacidad y protección de información de datos personales**	DE.DP-2	Definir las disposiciones para cumplir con la legislación de privacidad de los datos personales, ley estatutaria 1581 de 2012 y decreto 1377 que reglamenta la ley de 2013. 1) Definir una política para cumplir con la ley 2) Definir los responsables 3) Identificare los repositorios de datos personales 4) Solicitar consentimiento al titular para tratar los datos personales y guarda registro de este hecho. 5) Adoptar las medidas técnicas necesarias para proteger las bases de datos donde reposan estos datos.
A.18.2	**Revisiones de seguridad de la información**		
A.18.2.1	**Revisión independiente de la seguridad de la información**		Establecer revisiones independientes (por personas diferentes o no vinculadas a un proceso o área que se revisa), de la conveniencia, la adecuación y la eficacia continuas de la gestión a la seguridad de la información.
A.18.2.2	**Cumplimiento con las políticas y normas de seguridad**	PR.IP-12	1) Establecer auditorias para revisar que los coordinadores cumplan con todos los procedimientos de seguridad dentro de su área de responsabilidad se lleven a cabo correctamente para lograr el cumplimiento de las políticas y estándares de seguridad. 2) Revisar periódica del cumplimiento del centro de cómputo con las políticas y normas de seguridad establecidas. 3) Revisar regularmente los sistemas de información para asegurar el cumplimiento de las normas de seguridad de la información

Cuadro 10. . (Continuación)

ISO	DESCRIPCIÓN	NIST	PLAN DE ACCIÓN
A.18.2.3	**Revisión del cumplimiento técnico**	ID.RA-1	Documentar y realizar evaluaciones de seguridad técnicas por o bajo la supervisión de personal autorizado, apoyado en herramientas automáticas o con revisiones manuales realizadas por especialistas.

Fuente. Instrumento de Evaluación MSPI.

En este capitulo fue posible determinar los planes de acción, que se deben implementar para llevar a cabo los controles de la norma ISO/27001, su implementación de cada uno de estos planes determinara que se cuente con un sistema de seguridad de la información, el cual permitiría cumplir con la confidencialidad, la oportunidad e integridad de la información.

9 POLÍTICAS DE SEGURIDAD DE INFORMACIÓN

La políticas de seguridad, aborda la necesidad de la implementación de un sistema de gestión de seguridad de la información (SGSI) planteado desde la descripción del quién, qué, por qué, cuándo y cómo, en torno al desarrollo de la implementación del SGSI.

Es así como, teniendo en cuenta la importancia que tiene que la entidad defina las necesidades de sus grupos de interés, y la valoración de los controles precisos para mantener la seguridad de la información, se debe establecer una política que tenga en cuenta el marco general del funcionamiento de la entidad, sus objetivos institucionales, sus procesos misionales, y que este adaptada a las condiciones específicas y particulares de cada una según corresponda para que sea aprobada y guiada por la Dirección.

De esta forma, una buena política es concisa, fácil de leer y comprender, flexible y fácil de hacer cumplir para todos aquellos dentro del alcance sin excepción. Son cortas, y enmarcan los principios que guían las actividades dentro de la entidad.

Con base a los anteriores perceptos se realiza construcción de las siguientes políticas de seguridad de la información.

9.1 POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN.

La EPS INDÍGENA MALLAMAS, se compromete a: Proteger los activos de información de la organización, orientando sus esfuerzos a la preservación de la confidencialidad, integridad, disponibilidad, a la continuidad de las operaciones

propias de la organización, la administración y/o gestión de riesgos, la creación de cultura y conciencia de seguridad en los funcionarios, contratistas, proveedores y personas que hagan uso de los activos de información de MALLAMAS EPS - I, tomando como base que la efectividad de esta política depende finalmente del comportamiento de cada uno de los colaboradores y demás personas que puedan interactuar con el Sistema de información.

La EPS - I MALLAMAS es la propietaria de la información. Su tenencia y manejo es delegada a sus colaboradores, quienes son responsables de la custodia de la información que los procesos organizacionales generan, considerando su propósito y uso. Por ello los colaboradores deben ser conscientes de los riesgos a la que está expuesta la información a su cargo.

Esta política será revisada anualmente, o cuando se identifiquen cambios en la organización, o alguna condición que afecte la política, para asegurar que sigue siendo adecuada y ajustada a los requerimientos identificados.

9.1.1 Objetivo.

Definir medidas tendientes para una adecuada protección y seguridad de la información producida por los diferentes procesos de MALLAMAS EPS - I, evitando su posible pérdida por diferentes amenazas latentes.

9.1.2 Alcance.

Estas políticas se aplican a cada uno de los procesos organizacionales y a todos los datos generados por los distintos activos de información de información de MALLAMAS EPS - I.

9.1.3 Criterios.

- Se debe verificar que se definan, implementen, revisen y actualicen las políticas de seguridad de la información.

- Informar de los eventos que estén en contra de la seguridad de la información y de la infraestructura tecnológica de la EPS - I MALLAMAS.

- Todos los usuarios de los sistemas de información tienen la responsabilidad y obligación de cumplir con las políticas, normas, procedimientos y buenas prácticas de seguridad de la información establecidas en el presente manual.

- Permitir que se realicen las respectivas auditorías a la seguridad de la información.

- Todo aplicativo informático o software debe ser comprado o aprobado por la Dirección de Sistema de Información con el fin de verificar la funcionalidad, cumplimiento de requisitos legales y requerimientos de infraestructura tecnología que puedan permitir su actualización y óptimo funcionamiento.

- La EPS-I MALLAMAS debe contar con un firewall el cual limite los ataques externos, permitiendo exclusivamente el ingreso a los usuarios autorizados.

- Se debe contar con una red VPN (Virtual Private Network) lo cual permite el ingreso externo de forma segura a los aplicativos del Sistema de Información.

- Los jefes, directores y Coordinadores deben asegurarse de que todos los procedimientos de seguridad de la información se ejecuten y cumplan adecuadamente.
- Las políticas de seguridad de información se revisarán una vez al año con el objetivo de mejorar continuamente los procesos de seguridad, confidencialidad, integridad y disponibilidad de la información.

- Únicamente se permitirá el uso de software autorizado que haya sido adquirido legalmente por la organización o que se trate de software libre.

- Es responsabilidad de todos los funcionarios de la EPS - I MALLAMAS es reportar los incidentes de seguridad, eventos sospechosos y el mal uso de los recursos que identifique.

- La EPS - I MALLAMAS contará con un Plan de Continuidad del Negocio que asegure la continuidad de las operaciones, ante la ocurrencia de eventos no previstos o desastres naturales.

- Todo empleado es responsable de preservar la confidencialidad, integridad y disponibilidad de los activos de información en cumplimiento de la presente política y de las políticas y procedimientos inherentes a la seguridad de la información.

9.2 POLÍTICA DE CONTROL DE ACCESO

9.2.1 Objetivo.

Proporcionar seguridad razonable con respecto a los sistemas y recursos de información, a través de un adecuado manejo y mantenimiento de las cuentas de usuario, derechos y privilegios asociados, para acceder a servidores, aplicaciones, bases de datos, archivos empresariales y a las instalaciones de procesamiento de información de la EPS INDÍGENA MALLAMAS.

9.2.2 Alcance.

Esta política aplica a todos los sistemas de información, bases de datos, equipos informáticos, instalaciones y redes que la EPS Indígena MALLAMAS posee en la actualidad o en el futuro.

9.2.3 Criterios.

- Registrar la entrada y salida de los colaboradores del área de procesamiento de información.

- La Coordinación de Informática asigna los roles a cada colaborador dependiendo del cargo con el fin de controlar el ingreso al sistema de información.

- Los operadores sólo pueden acceder a información para la que están expresamente autorizados por el dueño del activo.

- Cuando un empleado deja algún puesto en la entidad, los archivos residentes en los computadores deben ser revisados por el jefe inmediato, para una inmediata reasignación formal de obligaciones y responsabilidades.

- Los Funcionarios de la organización no deben utilizar herramientas para obtener información de la red, como detección de puertos, servicios y archivos en general que sean propiedad de la EPS - I MALLAMAS.

- Las contraseñas no deben ser escritas o almacenadas en lugares visibles o cerca de los sistemas de información a los cuales permiten el acceso.

- Es responsabilidad del trabajador el manejo apropiado a las claves asignadas para acceso a los sistemas de información, estas claves de acceso y usuarios son personales e intransferibles.

- La Coordinación de Informática establecerá la forma de registro, cancelación y periodicidad de revisión y ajuste a permisos de acceso a los sistemas de información, asignados a los trabajadores, tomando como base los cambios que puedan presentarse dentro de las áreas previo aviso de la coordinación de Gestión Humana.

- Antes de otorgar los permisos de trabajo remoto a Funcionarios de la organización, se debe firmar un acuerdo de confidencialidad que proteja la información sensible de la organización.

- Todo acceso a los puertos de comunicaciones debe ser estrictamente controlado. Cualquier Usuario que requiera establecer una conexión interna o externa debe obtener aprobación de la Direccion de sistema de información o la coordinación de informática.

- La Dirección de Sistemas de Información debe mantener registros exactos y actualizados de todos los canales de comunicación de datos abiertos.

- Toda conexión remota donde el Usuario haya introducido 3 (tres) intentos fallidos de identificación y Contraseña errónea, debe ser inmediatamente desconectada.

9.3 POLÍTICA DE ACCESO A REDES Y SERVICIOS DE RED

9.3.1 Objetivo.

Garantizar el acceso de forma segura y controlada a los servicios de red implementados en la EPS INDÍGENA MALLAMAS.

9.3.2 Alcance.

Esta política aplica a todos los servicios de red con los que cuenta la EPS Indígena MALLAMAS.

9.3.3 Criterios.

- La Coordinación de Informática, implementara herramientas para evitar la descarga de software no autorizado y/o código malicioso en los equipos institucionales.

- Los funcionarios de la EPS - I MALLAMAS tiene restringido el acceso a redes sociales. En caso de ser requerido se debe solicitar mediante ORFEO a la Dirección de Sistemas de Información.

- La descarga de archivos de Internet debe ser con propósitos laborales y de forma razonable para no afectar el servicio.

- Las conexiones remotas a la red de la entidad se deben hacer mediante redes VPN (Virtual Private Network) seguras, suministradas por la EPS - I MALLAMAS.

- La información almacenada en las carpetas de los servidores de archivos debe ser de carácter institucional.

- Se prohíbe almacenar información no relacionada con las funciones asignadas al usuario, información personal, música, vídeos, películas, así como también archivos que puedan ocasionar o constituir riesgos informáticos, como software o código malicioso.

- Se prohíbe extraer, divulgar o publicar información de los servidores de archivos o estaciones de trabajo, sin expresa autorización del propietario del activo.

- Los usuarios deberán emplear los puntos de red de datos, para la conexión de equipos de cómputo pertenecientes a la EPS - I MALLAMAS.

- La administración de los puntos de red de datos es responsabilidad de la Coordinación de Informática de la EPS - I MALLAMAS.

- Los documentos que se impriman deben ser de carácter institucional.

- Ningún usuario debe realizar labores de reparación o mantenimiento de las impresoras, en caso de presentarse alguna falla, esta se debe reportar a la Coordinación de Informática de la EPS - I MALLAMAS.

- Los usuarios del correo electrónico corporativo son responsables de evitar prácticas o usos que puedan comprometer la seguridad de la información.

- El servicio de correo electrónico debe utilizarse exclusivamente para las tareas propias de la función y no para otro fin.

- No está autorizado el envío de correos con contenido que atenten contra la integridad y dignidad de las personas y el buen nombre de la entidad.

- Cada usuario es responsable del contenido del mensaje enviado y de cualquier otra información adjunta al mismo.

- Todo usuario es responsable por la apertura de los mensajes cuyo origen sea desconocido y por lo tanto asume la responsabilidad y las consecuencias que puede ocasionar la ejecución de cualquier archivo adjunto. En estos casos no se debe contestar dichos mensajes, ni abrir los archivos adjuntos y se debe remitir a Coordinación de Informática de la EPS - I MALLAMAS.

9.4 POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIOS

9.4.1 Objetivo.

Definir una política de responsabilidad compartida, en la que se establezcan buenas prácticas para el orden y la limpieza en el puesto de trabajo, acompañadas de las políticas de seguridad de la Información enmarcada en el esfuerzo eficaz y la aceptación de responsabilidades en el manejo de activos de la entidad que estén a cargo del funcionario, logrando un ambiente seguro y propicio al cambio.

9.4.2 Alcance.

Esta Política, aplica a todos los colaboradores de la EPS - I MALLAMAS, que se les haya asignado un escritorio de trabajo, un equipo de cómputo y manejo de documentos físicos y/o digitales, su propósito es resguardar la información y los sistemas, apropiadamente, tanto a nivel interno como a nivel externo.

9.4.3 Criterios.

- Los equipos que tengan contacto con publico externo a la entidad deben ser ubicados de tal manera que impida ver la información de la pantalla.

- Se prohíbe tener sustancias o líquidos en su escritorio, que puedan dañar los equipos, así como la documentación.

- Se hará registro fotográfico del escritorio del funcionario infractor, en donde se encuentren cuadernos, información en papel, carpetas, monitores encendidos y demás objetos que incumplan con esta política, para tenerlo como soporte de las medidas correctivas y/o administrativas que se definan.

- Se entregará esta documentación y pruebas recolectadas de incumplimiento de la política a la jefatura de control interno para que sean ellos quien tomen los correctivos correspondientes.

- Todos los equipos de cómputo del personal de la EPS - I MALLAMAS deben estar configurados para bloquear su pantalla después de 20 minutos de inactividad.

- Todos los equipos de cómputo deben estar configurados con el protector de pantalla, el cual será definido por la Dirección de Sistemas de Información.

- Todos los equipos de cómputo de la EPS - I MALLAMAS deberán contar con usuario y contraseña de sistema operativo.

- No se debe dejar dispositivos de almacenamiento de información, como USB, CD, DVD, Discos Duros Externos, etc., al alcance de cualquier persona.

- Todos los Funcionarios de la organización, deben dejar siempre sus equipos bloqueados en caso de no estar en su lugar de trabajo, para ello se debe utilizar las teclas Cerrar sesión de inicio de Windows y bloquear el equipo con comandos como Control + Alt + Supr o la tecla de Windows + L

- Todos los equipos de cómputo de la EPS - I MALLAMAS, deben ser apagados por los funcionarios que los utilizan una vez que termine la jornada de trabajo.

- Desde el momento en que se realiza la entrega y asignación de un equipo de cómputo, la responsabilidad sobre el estado de este es totalmente del funcionario.

- Se prohíbe pegar autoadhesivos en las pantallas.

- El usuario, debe preocuparse por mantener su equipo en buenas condiciones de limpieza externa.

- Cerrar con llave la puerta de la oficina cuando el personal esté ausente por períodos prolongados.

- Todos los equipos de la entidad deben estar con la imagen de fondo de la EPS-I MALLAMAS.

- Los equipos de cómputo y lugares de trabajo podrán ser revisados y auditados por las áreas de control que determine la entidad, a fin de validar el cumplimiento de la presente política.

- Es responsabilidad de cada funcionario la protección de los sistemas de información a su cargo, por lo que debe asegurar físicamente su computador portátil con cables de seguridad en todo momento para evitar robos.

9.5 POLÍTICA DE USO DE LOS ACTIVOS

9.5.1 Objetivo.

Alcanzar y mantener la protección de los activos de información por medio de la asignación de roles y funciones

9.5.2 Alcance.

Esta política aplica a cada uno de los procesos organizaciones que puedan interactuar con el Sistema de información de la EPS INDÍGENA MALLAMAS

9.5.3 Criterios.

Los activos de información pertenecen al EPS INDÍGENA MALLAMAS y el uso de estos debe emplearse exclusivamente con propósitos laborales.

- Los colaboradores deberán utilizar únicamente los programas y equipos autorizados por la Gerencia y la Dirección de Sistemas de Información.

- La EPS INDÍGENA MALLAMAS proporcionará a los colaboradores, los equipos informáticos y los programas instalados en ellos los datos/información creados, almacenados y recibidos, serán propiedad de la EPS INDÍGENA MALLAMAS, los funcionarios solo podrán realizar backup de sus archivos personales o de información pública, para copiar cualquier tipo de información clasificada o reservada debe pedir autorización a su jefe inmediato, de acuerdo a las normas sobre clasificación de la información de acuerdo a los niveles de seguridad establecidos Su copia, sustracción, daño intencional o utilización para fines distintos a las labores propias de la Institución, serán sancionadas de acuerdo con las normas y legislación vigentes.

- Periódicamente, la Coordinación de Informática efectuará la revisión de los programas utilizados en cada dependencia. La descarga, instalación o uso de aplicativos o programas informáticos NO autorizados será considera como una violación a las Políticas de Seguridad de la organización.

- Todos los requerimientos de aplicativos, sistemas y equipos informáticos deben ser solicitados por Jefes, Directores y Coordinadores a la Dirección de Sistema de Información.

- Estarán bajo custodia de la Coordinación de Informática los medios magnéticos/electrónicos (CDs u otros) que vengan originalmente con el software y sus respectivos manuales y licencias de uso, adicionalmente las claves para descargar el software de fabricantes de sus páginas web o sitios en internet y los passwords de administración de los equipos informáticos, sistemas de información o aplicativos.

- Los funcionarios no deben realizar intencionalmente actos que impliquen un mal uso de los recursos tecnológicos o que vayan en contravía de las políticas de seguridad de la información entre ellos envíos o reenvíos masivos de correos

electrónicos o spam, practica de juegos en línea, uso permanente de redes sociales personales, conexión de periféricos o equipos que causen molestia a compañeros de trabajo, etc.

- Los funcionarios no podrán efectuar ninguna de las siguientes labores sin previa autorización de la Dirección de Sistemas de Información.
- Instalar software en cualquier equipo

- Bajar o descargar software de Internet u otro servicio en línea en cualquier equipo.

- Modificar, revisar, transformar o adaptar cualquier software propiedad de la entidad.

- Descompilar o realizar ingeniería inversa en cualquier software de propiedad de la entidad.

- Copiar o distribuir cualquier software de propiedad de la entidad.

- Cambiar la configuración de hardware de propiedad de la entidad.

- El funcionario será responsable de todas las transacciones o acciones efectuadas con su cuenta de usuario.

- Ningún funcionario deberá acceder a la red o a los servicios TIC de la EPS INDÍGENA MALLAMAS, utilizando una cuenta de usuario o clave de otro usuario.

- Los funcionarios no están autorizados para hacer uso de redes externas a través de dispositivos personales en las instalaciones de la entidad (modem USB,

router, wifi público, etc.), esto compromete la seguridad de los recursos informáticos de la EPS INDÍGENA MALLAMAS.

- La Coordinación de Informática, es el área responsable de realizar el aseguramiento de los accesos a internet, acceso a redes de terceros y a las redes de la entidad esta responsabilidad incluye, pero no se limita a prevenir que intrusos tengan acceso a los recursos informáticos y a prevenir la introducción y propagación de virus.

- La información de la EPS INDÍGENA MALLAMAS debe ser respaldada de forma frecuente, debe ser almacenada en lugares apropiados en los cuales se pueda garantizar que la información está segura y podrá ser recuperada en caso de un desastre o de incidentes con los equipos de procesamiento.

Los funcionarios deberán realizar la devolución de todos los activos físicos y/o electrónicos asignados por la EPS INDÍGENA MALLAMAS en el proceso de desvinculación.

9.6 POLÍTICA DE PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS

9.6.1 Objetivo.

Contar con una plataforma de hardware y software que proteja la integridad y disponibilidad de la información y del software que la procesa. La red local de MALLAMAS EPS-I, de malware, troyanos, y demás virus que atenten contra la integridad y disponibilidad de la información almacenada tanto en servidores como en estaciones de trabajo y cualquier otro medio magnético.

9.6.2 Alcance.

Aplica a todos los procesos organizacionales que generen algún tipo de información

9.6.3 Criterios.

- **Controles contra código malicioso**

Se deberán tomar las precauciones necesarias para proteger la red local de MALLAMAS EPS-I previniendo, detectando y recuperándose de la introducción de software malicioso como son virus en las PC´s y Servidores, Caballos de Troya, Gusanos en la Red y bombas lógicas.

- Se deberán tomar en cuenta la concientización de los usuarios en cuanto a los controles contra software malicioso con que cuenta la organización, los apropiados accesos a sistemas y el control de cambios.

- Prescindir de instalar software no autorizado.

- No descargar software ni aplicaciones desde Internet sin previa autorización de la coordinación de informática

- La red de servidores y computadores de MALLAMAS EPS INDÍGENA deberá tener instalada una plataforma de hardware y software de antivirus para evitar la propagación de virus a través de archivos externos obtenidos de otras redes.

La plataforma de Antivirus deberá cumplir con los siguientes requerimientos:

- Consola centralizada de administración.
- Actualización de DAT permanente, automática y centralizada.
- Distribución de actualizaciones automáticas de las estaciones de trabajo.
- Monitoreo centralizado.
- Alto grado de detección (comprobado).
- Bajo impacto en los tiempos de respuesta de las estaciones.

- Proteger el total de computadores y servidores de la red de la EPS INDÍGENA MALLAMAS
- Capaz de correr en las distintas plataformas existentes en la institución (Windows, Linux, otros).
- Alarma centralizada de brotes de virus.
- Soporte centralizado de la herramienta en caso de ser necesaria la consulta a terceros. (teléfono ayuda y/o contrato soporte presencial)
- Entrega de información de cada equipo que tenga instalada la herramienta (dirección IP, procesador, sistema operativo, disco, RAM, etc.)
- Se deberá realizar en forma periódica una revisión silenciosa de virus en los equipos informáticos, para evitar la propagación de estos, como medida preventiva.
- Se deberá hacer una revisión diaria del funcionamiento del sistema de gestión de antivirus.
- En caso de que surja un problema con virus en algún equipo informático deberá seguirse un procedimiento de recuperación de ataques de virus y código malicioso.
- La coordinación de informática deberá estar suscrita a los boletines de alerta tanto del fabricante como del proveedor del antivirus, así como de los principales fabricantes de antivirus en el mercado, para determinar y seguir las recomendaciones de terceros en caso de ataques o vulnerabilidades, también para diferenciar y determinar los diversos riesgos o falsos virus.
- La herramienta de Antivirus que se implemente en la organización tendrá carácter de corporativo y por ende será obligatoria su instalación y uso en todo el equipamiento computacional sean estos servidores, estaciones de trabajo, notebook y otros dispositivos. Cualquier equipo que no cuente con esta protección de antivirus, no podrá ser conectado a la red de datos local de la institución.
- El antivirus debe instalarse en un computador con características mínimas que le permitan correr y cumplir su función y es de la coordinación de informática

quién valida que el equipo está en condiciones. Si no lo soporta, el equipo quedará sin posibilidades de conectarse a la red de datos.

- La configuración del antivirus propiamente dicha dependerá de los servicios que presta el equipamiento, quedando como responsable la coordinación de informática, determinar la mejor opción.
- Si bien el antivirus debe entregar alarmas por infecciones, para el caso en que sean los mismos usuarios quienes detecten las alarmas locales, deben ser estos quienes den aviso inmediatamente a la coordinación de informática vía telefónica o bien por correo electrónico

9.7 POLÍTICA PARA EJECUTAR COPIAS DE SEGURIDAD

9.7.1 Objetivo.

Garantizar la disponibilidad, seguridad y confidencialidad de la información Institucional de la Entidad mediante la gestión de las copias de respaldo y su recuperación cuando sea requerido. Para lo cual debe contar una periodicidad, confidencialidad, integridad y la disponibilidad de esta cuando esta sea requerida.

9.7.2 Alcance.

Esta política aplica para toda la información generada dentro de la organización

9.7.3 Criterios.

- Las jefaturas, Direcciones y coordinaciones deben solicitar a la coordinación de informática la asignación del espacio en el servidor con el fin de ubicar la información.

- Una vez asignado el espacio en el servidor se define usuario y contraseña y los usuarios que pueden ingresar y modificar la información.

- Las copias de seguridad se realizarán con una frecuencia determinada teniendo en cuenta la criticidad de la información, estas copias quedarán almacenadas en el servidor de la EPS-I MALLAMAS.

- Garantizar la custodia y almacenamiento de los medios en una Entidad externa a la EPS-I MALLAMAS, donde se garantice la seguridad e integridad de la información.

- Para solicitar una copia de información ya sea por consulta o por perdida el jefe, director o coordinador solicitara a la coordinación de informática a través del formato establecido para tal fin.

- No se podrá almacenar en los servidores de la Entidad información de índole personal o que no corresponda a la legalmente autorizada, cumpliendo con la normatividad relacionada con derechos de autor.

- La coordinación de informática monitorea regularmente los registros de logs y eventos de las herramientas, junto con los procedimientos de los backups realizados. En caso de encontrar alguna alarma o sospecha de la calidad del backup, se debe repetir y hacer seguimiento para corregir las fallas detectadas.

- La realización de los backups, se deben programar en horario nocturno, esto con el fin de no causar traumatismos en la realización de este proceso.

9.8 POLÍTICA PARA LA TRANSFERENCIA DE INFORMACIÓN

9.8.1 Objetivo.

Proteger la información transferida al interior de la EPS INDÍGENA MALLAMAS

9.8.2 Alcance.

Aplica para toda la información interna y externa

9.8.3 Criterios.

- La organización realizará transferencia de información con organizaciones gubernamentales y privadas, basados en la necesidad de la Entidad que permita automatizar servicios, fortaleciendo la gestión de la EPS INDÍGENA MALLAMAS.

- La organización generará acuerdos de transferencia de información, previa solicitud a la coordinación de informática.

- La transferencia de información deberá determinarse a través de un convenio interadministrativo o contrato, el acuerdo de transferencia debe realizarse siguiendo lo establecido en el Manual de Contratación.

- - La transferencia de información al interior de la organización se realizará a través de los medios oficiales de comunicación.

- La Transferencia de información en medio físico se realizará de acuerdo con lo establecido por la organización en el Programa de Gestión Documental

- La Transferencia de información digital

- La coordinación de informática implementará las herramientas seguras para la transferencia de información al interior de la organización.

- La coordinación de informática debe implementar las herramientas necesarias para asegurar la transferencia de información al interior y exterior de la EPS INDÍGENA MALLAMAS contra interceptación, copiado, modificación, enrutado y destrucción.

- La coordinación de informática deberá controlar las acciones para reenvío automático de correo electrónico a direcciones de correo externo.

- La coordinación de informática realizara el control del uso de sistemas de transferencia de archivos vía FTP a terceros.

9.9 POLÍTICA DE SEGURIDAD PARA RELACIÓN CON PROVEEDORES

9.9.1 Objetivo.

Garantizar la información que se produce entre MALLAMAS EPS I y los proveedores

9.9.2 Alcance.

Esta política aplica para la información que se genera entre MALLAMAS EPS-I Y los diferentes proveedores

9.9.3 Criterios.

- No divulgar las condiciones generales de contratación a terceros.

- Desarrollar las actividades comerciales teniendo en cuenta los lineamientos de software establecidos por MALLAMAS EPS-I.

- Toda información que se genere entre MALLAMAS EPS-I y los diferentes proveedores sea veraz.

- Verificar toda la información suministrada por parte de los proveedores sea veraz.

- Suministrar información de MALLAMAS EPS-I solo cuando se requiera

9.10 POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES

9.10.1 Objetivo.

Garantizar que la EPS INDÍGENA MALLAMAS, actúe como responsable del tratamiento de sus datos personales y hará uso de estos únicamente para las finalidades para las que se encuentra facultada

9.10.2 Alcance.

Esta política aplica para la información que maneja la EPS MALLAMAS EPS-I en cuanto a sus afiliados, funcionarios y proveedores.

9.10.3 Criterios.

9.10.3.1 Modo en que se utiliza la información.

Previa autorización del titular de los datos personales le permitirá a la EPS INDÍGENA MALLAMAS dar el siguiente tratamiento:

- Para los fines administrativos propios de la entidad

- Caracterizar ciudadanos y grupos de interés y adelantar estrategias de mejoramiento en la prestación del servicio

- Dar tratamiento y respuesta a las peticiones, quejas, reclamos, denuncias, sugerencias presentadas a la organización

- Alimentar el Sistema de Información

- Conocer y consultar la información del titular del dato que reposen en bases de datos de entidades públicas o privadas

- Adelantar encuestas de satisfacción y percepción de los grupos de valor

- Envío de información de interés general

9.10.3.2 Derechos de los titulares de los datos personales.

La EPS-I MALLAMAS, garantizara al titular de datos personales, el pleno ejercicio de los derechos que se enlistan a continuación:

- Conocer, actualizar y rectificar sus datos personales. Este derecho se podrá ejercer también, frente a datos parciales, inexactos, incompletos, fraccionados, que

induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado.

- Solicitar prueba de la autorización otorgada a la EPS-I MALLAMAS para el tratamiento de sus datos personales.

- Ser informado del uso y tratamiento dado a sus datos personales, previa solicitud elevada a través de los canales de servicio.

- Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la ley y las demás normas que la modifiquen, adicionen o complementen.

- Revocar la autorización y/o solicitar la supresión de uno a más datos cuando en el tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el tratamiento de los datos se ha incurrido en conductas contrarias a la ley y a la Constitución.

- Acceder en forma gratuita a sus datos personales que hayan sido objeto de tratamiento.

Como se ha determinado la importancia de las políticas de seguridad de la información, se sugiere se realice la implementación de las misma, las cuales es necesario contar con la aprobación de la alta dirección, así como el comité de seguridad, el cual permitirá vigilar, su cumplimiento, así como determinar su revisión y actualización de requerirse.

CONCLUSIONES

En este aparte se presenta las conclusiones, producto del análisis de la problemática desarrollada en el presente trabajo, en donde se destacan aspectos importantes de cada uno de los objetivos logrados, para lograr esa planificación del sistema de gestión de seguridad de la información planteado.

La importancia de conocer como las metodologías existentes de recolección de información, como la que otorga el Ministerio de las TIC, brindan un horizonte mediante el cual es posible realizar un diagnóstico de cómo se encuentra las entidades en materia de seguridad de información, con base en esta información es viable direccionar los proyectos, que permite de manera correcta conocer y clasificar la información que consideramos importante, además que integra a esta metodología el framework de buenas prácticas de seguridad como es las NITS.

Realizar un inventario de los activos a través de su identificación y poder mediante las metodologías MAGERIT, desarrollada en el presente proyecto, permite conocer de manera más fácil los riesgos, cuantificar su valor, e identificar las vulnerabilidades de acuerdo con las amenazas, además nos proporciona de cómo se puede valorar estas amenazan, lo cual es concluyente para poder tomar las medidas necesarias que conlleven a mitigar, eliminar, transferir hasta en algunos casos aceptarlo los riesgos de la manera más objetiva posible.

La importancia de asociar los riesgos y poder realizar los controles para cada uno de ellos, a través del anexo técnico A de la Norma ISO 27001:2013, mancomunado a las buenas prácticas establecidas por la NITS, permite tomar las acciones necesarias, para una buena gestión de estos riesgos que como resultado logran tener un buen sistema de gestión de seguridad de la información.

Al incorporar los planes de acción o recomendación realizadas a los controles es necesario el establecimiento de políticas de seguridad de la información, para aquellos procedimientos importantes de la entidad y que son de estricto cumplimiento por parte de la normatividad ISO 27001:2013, los que permite crear las reglas necesarias, las cuales, a través de una buena divulgación y concientización, aporta de gran manera el cumplimiento de los objetivos del sistema de gestión de información.

RECOMENDACIONES

Después de dar cumplimiento a los objetivos propuestos y en base a las conclusiones obtenidas, realizamos las siguientes recomendaciones.

Para que un sistema de seguridad de la información sea implementado con éxito, es necesario contar con el compromiso en cabeza de la dirección de la entidad, así mismo de cada uno de los funcionarios que intervienen en el proceso. Por lo cual es importante continuar con esta iniciativa por parte del área de tecnología de la entidad que permita implementar las siguientes etapas, para su culminación.

La comunicación, la comprensión, y sensibilización son los factores importantes, para llevar a cabo el cumplimiento de todas las políticas de seguridad de la información que la organización establezca, para lo cual esta debe estar presente en cada proceso de inducción y reinducción de los funcionarios.

Realizar las auditorías internas necesarias, que permitan a la organización establecer planes de mejoramiento a los hallazgos realizados, la revisión de las políticas y de los controles implementados, garantizara la mejora continua en la gestiona de los riesgos y de esta manera garantizar la seguridad de la información. Por lo que es importante que el comité de seguridad de la información que se va a establecer tenga como una de sus iniciativas establecer estas auditorias que permitirán el mejoramiento continuo.

BIBLIOGRAFÍA

27001ACADEMY. ¿Qué es norma ISO 27001?. [Sitio web]. [Consulta: 26 de Marzo de 2021]. Disponible en: https://advisera.com/27001academy/es/que-es-iso-27001/#:%7E:text=ISO%2027001%20es%20una%20norma,ISO%2FIEC%202700 1%3A201327001/#:~:text=ISO%2027001%20es%20una%20norma,ISO%2FIEC% 2027001%3A2013.

COLOMBIA, CONGRESO DE LA REPUBLICA. Ley Estatutaria 1266 de 2008, 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. En; Diario oficial. Diciembre 31 de 2008, Nro.47.219. p.3

COLOMBIA, CONGRESO DE LA REPUBLICA. 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. En; Diario oficial. Enero 5 de 2009, Nro.47.223. p.5

COMISIÓN DE REGULACIÓN DE COMUNICACIONES. Resolución 2258 de 2009, Por la cual se modifican los artículos 22 y 23 de la Resolución CRT 1732 de 2007 y los artículos 1.8 y 2.4 de la Resolución CRT 1740 de 2007. En; Diario oficial. Diciembre 23 de 2009, Nro.47.572. p.8

EALDE BUSINESS SCHOOL. Metodologías en Gestión de Riesgos. [Sitio web]. [Consulta: 25 de Marzo de 2021]. Disponible en: https://www.ealde.es/metodologias-gestion-riesgos/

FIRMA-E. Pilares de la Seguridad de la Información: confidencialidad, integridad y disponibilidad [Sitio web]. [Consulta: 26 de Marzo de 2021]. Disponible en: https://www.firma-e.com/blog/pilares-de-la-seguridad-de-la-informacion-confidencialidad-integridad-y-disponibilidad/

ICONTEC. Quiénes somos. [Sitio web]. [Consulta: 26 de Marzo de 2021]. Disponible en: https://www.icontec.org/quienes-somos/

GOBIERNO DIGITAL. MSPI. Modelo de Seguridad y Privacidad de la Información. [Sitio web]. Bogotá D.C. [Consulta: 26 de Marzo de 2021]. Disponible en: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/

MALLAMAS EPS INDÍGENA, Reseña Histórica, [Sitio Web] Ipiales – Nariño [Consultado el 28 de Marzo de 2021] Disponible en: https://www.mallamaseps.com.co/index.php/component/k2/item/3-resena-historica#:~:text=MALLAMAS%20EPS%20INDIGENA%2C%20nace%20por,hacia%20el%20a%C3%B1o%201996%20por

MALLAMAS EPS INDÍGENA, Plataforma estratégica, [Sitio Web] Ipiales – Nariño [Consultado el 28 de Marzo de 2021] Disponible en: https://www.mallamaseps.com.co/index.php/nosotros/plataforma

OSTEC . Segurança digital de resultados . ISO 27002: Buenas prácticas para gestión de la seguridad de la información. [Sitio web]. [Consulta: 26 de Marzo de 2021]. Disponible en: https://ostec.blog/es/generico/iso-27002-buenas-practicas-gsi/

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PUBLICAS. Subdirección General de Información, Documentación y Publicaciones. 2012. MAGERIT – versión 3.0 .Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método. Magerit 3.0. Madrid. España. P. 22

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PUBLICAS .Subdirección General de Información, Documentación y Publicaciones. 2012. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos. Magerit 3.0. Madrid. España P. 25-47

RUGE PINZÓN, Jeison Nicolas. Metodología para identificación y valoración de riesgos y salvaguardas en una mesa de ayuda tecnológica. [en línea]. Trabajo de grado. Universidad piloto de Colombia. Bogotá D.C.: 2011. [Consultado 28, marzo,2021]. Disponible en: http://polux.unipiloto.edu.co:8080/00000744.pdf

SUPERINTENDENCIA FINANCIERA, Boletín Ministerio de Hacienda, Capítulo Superintendencia Financiera de Colombia, No. 76 de 25 de octubre de 2007. Circular Externa 052 de Octubre de 2007 [Sitio Web] [Consultado el 28 de Marzo de 2021] Disponible en: https://normativa.colpensiones.gov.co/colpens/docs/circular_superfinanciera_0052_2007.htm

WIKIPEDIA LA ENCICLOPEDIA LIBRE. Sistema de gestión de la seguridad de la información. [Sitio web]. [Consulta: 25 de Marzo de 2021]. Disponible en: https://es.wikipedia.org/wiki/Sistema_de_gesti%C3%B3n_de_la_seguridad_de_la_informaci%C3%B3n

WIKIPEDIA LA ENCICLOPEDIA LIBRE. Información. Wikipedia, la enciclopedia libre. [Sitio web]. [Consulta: 25 de Marzo de 2021]. Disponible en: https://es.wikipedia.org/wiki/Informaci%C3%B3n#:%7E:text=Informaci%C3%B3n%

20es%20el%20nombre%20por,sistema%20que%20recibe%20dicho%20mensaje.&text=En%20biolog%C3%ADa%2C%20la%20informaci%C3%B3n%20se,al%20comportamiento%20de%20los%20individuos

WIKIPEDIA LA ENCICLOPEDIA LIBRE. Seguridad de la información. [Sitio web]. [Consulta: 25 de Marzo de 2021]. Disponible en: https://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n

WIKIPEDIA LA ENCICLOPEDIA LIBRE. Organización Internacional de Normalización. Wikipedia, la enciclopedia libre. [Sitio web]. [Consulta: 26 de Marzo de 2021]. Disponible en: https://es.wikipedia.org/wiki/Organizaci%C3%B3n_Internacional_de_Normalizaci%C3%B3n

ANEXOS

Anexo A Autorización de la Organización

Ipiales, 27 de Marzo de 2021

Doctor
Fabio Edmundo Enríquez Miranda
Gerente General

Asunto: Autorización para la ejecución del proyecto titulado: DISEÑO DE LA ETAPA DE PLANIFICACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN EL PROCESO DE GESTIÓN DE RECURSOS FÍSICOS Y TECNOLÓGICOS DE LA EMPRESA INDÍGENA MALLAMAS.

Cordial saludo estimado Gerente,

Como es de su conocimiento, actualmente me encuentro adelantando estudios de posgrado en la Especialización en Seguridad Informática ofertado por la Universidad Nacional Abierta y a Distancia "UNAD". Para finalizar mi proceso académico es mi objetivo desarrollar un trabajo de grado aplicado a *MALLAMAS EPS INDÍGENA*, de manera que pueda aportar mis conocimientos adquiridos y generar un impacto positivo en la empresa, relacionado con los temas de Seguridad Informática, motivo por el cual, muy comedidamente solicito su autorización y aprobación para la ejecución del proyecto titulado: *DISEÑO DE LA ETAPA DE PLANIFICACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN EL PROCESO DE GESTIÓN DE RECURSOS FÍSICOS Y TECNOLÓGICOS DE LA EMPRESA INDÍGENA MALLAMAS* el cual se encuentra avalado por parte la Institución de educación superior "UNAD". El proyecto en su objetivo general describe lo siguiente:

Diseñar la etapa de planificación de un sistema de gestión de seguridad en la información en el proceso de Gestión de Recursos Físicos y Tecnológicos, basados en el estándar de la norma ISO/IEC 27001:2013, la gestión de los riesgos; al mismo tiempo será apoyado por los objetivos específicos:

- Identificar el contexto de la organización en cuanto a la seguridad de la información basado en un instrumento MSPI del ministerio de las TIC.
- Analizar los riesgos de seguridad que se encuentra asociados a cada activo de información pertenecientes al proceso gestión de recursos físicos y tecnológicos mediante la adopción de una metodología de riesgo
- Definir los controles a los riesgos de seguridad de la información con base en guía de buenas prácticas de la ISO/IEC 27002:2013
- Elaborar la política de seguridad de la información que permita gestionar los riesgos para la EPS MALLAMAS

para obtener como resultado un alto impacto en la seguridad de la empresa *MALLAMAS EPS INDÍGENA*

De obtener esta autorización, se elaborará un acuerdo de confidencialidad para proteger la identidad la empresa y sus activos de información; a su vez se destacan los siguientes procesos para ser garantes en la transparencia de la ejecución del proyecto:

Anexo B Autorización de la Organización

- Se prohíbe la ejecución de cualquier tipo de pruebas de seguridad que no estén autorizadas expresamente por *MALLAMAS EPS INDÍGENA*
- La empresa *MALLAMAS EPS INDÍGENA* deberá establecer qué tipo de información es privada y cuál es pública para delimitar el acceso de pruebas en la ejecución del proyecto.
- La solicitud de información al igual que ejecución de pruebas deben quedar por escrito y se genera un informe de resultados semanalmente el cual será compartido con el gerente de la organización o empresa.
- La persona autorizada siempre debe operar dentro de la ley 1273 de 2009 y de las demás regulaciones establecidas en la empresa.
- Respetar la privacidad de todos los individuos y mantener su privacidad en los reportes. Se encuentra prohibida la divulgación de información personal en tales reportes.

El resultado del proyecto se verá reflejado en un documento el cual será cargado al repositorio institucional de la Universidad Nacional Abierta y a Distancia "UNAD". El documento ampara la confidencialidad y anonimato de la empresa, estos aspectos se encuentran estipulados en el acuerdo de confidencialidad; agradezco el apoyo prestado en esta etapa de mi carrera profesional.

Firman en Ipiales Nariño, a los (27) días del mes de (Marzo) de 2021

Cordialmente.

CRISTIAN PORTILLA
Estudiante UNAD.

FABIO ENRÍQUEZ MIRANDA
Gerente General

Anexo C RAE

Fecha de Realización:	05/10/2021
Programa:	ESPECIALIZACIÓN DE SEGURIDAD INFORMÁTICA
Línea de Investigación:	PROYECTO APLICADO
Título:	DISEÑO DE LA ETAPA DE PLANIFICACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN EL PROCESO DE GESTIÓN DE RECURSOS FÍSICOS Y TECNOLÓGICOS DE LA EPS INDÍGENA MALLAMAS
Autor(es):	CRISTHIAN BARNY PORTILLA MARTÍNEZ
Palabras Claves:	SGSI, Riesgos, MSPI, ISO27001, Seguridad
Descripción:	En el presente, se documenta la realización de etapa de planificación de un sistema de gestión de seguridad en la información en el proceso de gestión de recursos físicos y tecnológicos, de la empresa MALLAMAS EPS INDÍGENA, que posibilite garantizar los principios básicos como, la integridad, confidencialidad y la disponibilidad, el manejo de políticas de seguridad en la información, al igual un inventario de activos que permita una gestión de riesgo adecuada. Esta etapa se realizó mediante el levantamiento de un inventario de activos, los cuales a través de la metodología MAGERIT, se realizó la gestión del riego, las cuales a través del marco de la ISO/IEC 27001:2013, al igual con su guía de buenas prácticas enmarcadas en la ISO/IEC 27002:2013, permitió establecer los controles correspondientes y establecer políticas de seguridad, que al final garantizará la

	integridad, confidencialidad y disponibilidad de la información

Fuentes bibliográficas destacadas:

FIRMA-E. Pilares de la Seguridad de la Información: confidencialidad, integridad y disponibilidad [Sitio web]. [Consulta: 26 de Marzo de 2021]. Disponible en: https://www.firma-e.com/blog/pilares-de-la-seguridad-de-la-informacion-confidencialidad-integridad-y-disponibilidad/

GOBIERNO DIGITAL. MSPI. Modelo de Seguridad y Privacidad de la Información. [Sitio web]. Bogotá D.C. [Consulta: 26 de Marzo de 2021]. Disponible en: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/

OSTEC . Segurança digital de resultados . ISO 27002: Buenas prácticas para gestión de la seguridad de la información. [Sitio web]. [Consulta: 26 de Marzo de 2021]. Disponible en: https://ostec.blog/es/generico/iso-27002-buenas-practicas-gsi/

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PUBLICAS. Subdirección General de Información, Documentación y Publicaciones. 2012. MAGERIT – versión 3.0 .Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método. Magerit 3.0. Madrid. España. P. 22

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PUBLICAS .Subdirección General de Información, Documentación y Publicaciones. 2012. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II- Catálogo de Elementos. Magerit 3.0 Madrid. España P25-47

RUGE PINZÓN, Jeison Nicolas. Metodología para identificación y valoración de riesgos y salvaguardas en una mesa de ayuda tecnológica. [en línea]. Trabajo de grado. Universidad piloto de Colombia. Bogotá D.C.: 2011. [Consultado 28, marzo,2021]. Disponible en: http://polux.unipiloto.edu.co:8080/00000744.pdf	
Contenido del documento:	En el presente documento encontraremos en sus primeros apartes, la contextualización del proyecto, en donde se realiza una breve introducción, se establece unos objetivos a cumplir, se realiza la referencia de los marcos metodológicos, normativos y contextuales. Posteriormente encontraremos un capítulo en donde se describirá el diagnóstico de la empresa de cómo se encuentra actualmente, el cual se realizó mediante el uso del Modelo de Seguridad y Privacidad de la Información del ministerio de las TIC, a través de guías de evaluación. Posteriormente se realiza la gestión de riesgo mediante el inventario de activos través de la metodología MAGERIT, Cuyos resultados en el siguiente capitulo se realizan los controles correspondientes a través del anexo técnico A de la norma ISO27001:2013 y el manejo de actividades a través del framework de buenas prácticas de NITS. Por último, se encuentran algunas de las políticas que se sugieren ser implementadas, producto de la realización de los objetivos del proyecto.
Marco Metodológico:	La metodología descriptiva fue utilizada para llevar a cabo la etapa de planificación de un sistema de gestión de seguridad en la información, teniendo en cuenta que es necesario conocer el contexto actual de la

	organización, permitiendo la descripción de esto de forma sistémica, en donde gracias a esta metodología se realizó un análisis, a través de la recolección de información, que permitió describir e interpretar todo lo anterior basado en el marco de trabajo de la ISO/IEC27001/:2013, así como la adopción de la guía de buenas prácticas establecidas en la ISO/IEC 27002:2013.
Conceptos adquiridos :	En el presente proyecto fue posible conocer como las entidades públicas, cuentan con herramientas elaboradas por el ministerio de las TIC, como es el Modelo de Seguridad y Privacidad de la Información, el cual Proporciona los lineamientos para implementar y adoptar las buenas prácticas, de acuerdo con los estándares internacionales, para que incorporen la seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y, en general, en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos. Así mismos la metodología desarrollada por el Consejo Superior de Administración Electrónica en España. MAGERIT, en su versión 3, Proporciona herramientas de cuantificación, clasificación de los riesgos, los cuales brindan lineamientos claros, para poder gestionar los mismos de manera más objetiva. Igualmente, los controles que son posibles establecer mediante el anexo técnico A de la ISO27001:2013, son herramientas para poder mitigar los riesgos, que los

	cuales de la mano con el framework de NITS de ciberseguridad, se estable la incorporación de buenas prácticas, que permiten gestionar estos riesgos. Con todas las herramientas antes mencionas se facilita la incorporación en las empresas sistemas de gestión de seguridad de la información.
Conclusiones:	La importancia de conocer como las metodologías existentes de recolección de información que brindan un horizonte mediante el cual podamos realizar un diagnóstico de cómo se encuentra las entidades en materia de seguridad de información Realizar un inventario de los activos a través de su identificación y poder mediante las metodologías desarrolladas en el presente proyecto, es concluyente para poder tomar las medidas necesarias que conlleven a mitigar, eliminar, transferir hasta en algunos casos aceptarlos de la manera más objetiva posible. La importancia de asociar los riesgos y poder realizar los controles, a través del anexo técnico A de la Norma ISO 27001:2013, además de tener en cuenta las buenas prácticas establecidas por la NITS, ayuda de gran manera a poder tomar las acciones necesarias, que permite realizar una buena gestión de estos riesgos, los cuales, de tomar las medidas planteadas, se lograría tener un buen sistema de gestión de seguridad de la información.