DISEÑO DE SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION (SGSI) EN SALUD VIDA EPS NIVEL CENTRAL

SANDRA MILENA SIERRA ORTIZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA
INGENIERIA DE SISTEMAS
BOGOTA
2018

DISEÑO DE SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION (SGSI) EN SALUD VIDA EPS

SANDRA MILENA SIERRA ORTIZ

Informe Plan de trabajo práctica profesional Ingeniería de Sistemas

Docente acompañante de la práctica:

ING. IVAN ALEJANDRO VELOZA PEÑUELA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA
INGENIERIA DE SISTEMAS
BOGOTA

2018

CONTENIDO

LISTA DE ILUSTRACIONES

LISTA DE TABLAS

INTRODUCCION

La seguridad de la información busca garantizar la confidencialidad, la integridad y la disponibilidad de la información independientemente del formato en el que este consignada, llámese papel, video, imágenes, archivos, fotografías, datos, etc., puesto que no es exclusivamente de medios electrónicos sino que comprende el conjunto de datos que pueden ser la base de una compañía y que si llegan hacer manipuladas por manos inescrupulosas afectan la actividad tanto de un individuo como de una gran empresa llegando a causar hasta un gran impacto social.

En la actualidad los delitos informáticos que van en aumento se han convertido en la piedra en el zapato para muchas empresas, por lo que salvaguardar sus activos de información se vuelve obligatorio en cualquier compañía, para asegurar un adecuado control con respecto a riesgos a la información una de acciones más eficaces y económicas es la de implementar un sistema de gestión de seguridad de la información (SGSI), que permite llevar una serie de procesos sistemáticos y organizados para la planeación, ejecución, seguimiento y mejora del mismo; este sistema está basado en estándares, modelos y normas internacionales que a través de mejores prácticas aseguran una adecuada gestión de la seguridad de la información.

De acuerdo a lo anterior y teniendo en cuenta que como opción de grado de la carrera ingeniería de sistemas de la universidad Nacional Abierta y a distancia UNAD se ha realizado la pasantía en seguridad de la información en la empresa SALUDVIDA EPS. A continuación presentaré informe del proceso y resultados obtenidos del diseño de un sistema de gestión de seguridad de la información (SGSI) basado en las normas ISO/IEC 27001 teniendo como base

principal el plan de trabajo aprobado por el Comité Curricular del Programa Ingeniería de Sistemas.

En este documento encontrará la planificación del sistema de gestión de seguridad de la información que se compone de definición de alcance, políticas y metodología a utilizar, inventario de activos de la información, análisis de riesgos y vulnerabilidades frente a la seguridad de la información; con un tiempo de duración de 640 horas, distribuidas entre 48 horas semanales, iniciando desde el 19 de Julio hasta el 24 de septiembre del año en curso.

1. OBJETIVOS

1.1 OBJETIVO GENERAL

1.2 Apoyo a la gestión de seguridad de la información mediante el diseño de un sistema de gestión de seguridad de la información (SGSI) para Salud Vida EPS.

1.3 OBJETIVOS ESPECIFICOS

- Definir el alcance, políticas y metodología a utilizar.
- Inventario de activos de la información.
- Realizar un análisis de los riesgos y vulnerabilidades que pueda tener la organización frente a la seguridad de la información, esto permite determinar el nivel de seguridad actual en la organización y las posibles medidas a tomar.
- Revisar los controles ya existentes de seguridad de la información.
- Diseñar el Sistema de Gestión de Seguridad de la Información (SGSI)

2. MARCO CONCEPTUAL

Se presentan algunas definiciones importantes relacionadas al S GSI:

ACTIVOS DE INFORMACION: Los activos son los recursos que tiene un valor para el Sistema de Seguridad de la Información, necesarios para que la empresa funciones y consiga los objetivos que se ha propuesto la alta dirección.

AMENAZA: Se puede definir como amenaza a todo elemento o acción capaz de atentar contra la seguridad de la información.

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

ATAQUE INFORMATICO: Es un intento organizado e intencionado causada por una o más personas para causar daño o problemas a un sistema informático o red.

AUDITORÍA: proceso sistemático, independiente y documentado para obtener evidencias de auditoria y para determinar el grado en el que se cumplen los criterios de auditoria. (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).

BASE DE DATOS: conjunto organizado de datos personales que sea objeto de Tratamiento. (Fuente: Ley Estatutaria 1581 del 17 de octubre de 2012).

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: propiedad de la información de no ponerse a disposición o ser revelada a personas, entidades o procesos no autorizados.

CONSENTIMIENTO INFORMADO DEL TITULAR: es una manifestación de la voluntad, informada, libre e inequívoca, a través de la cual el titular de los datos de carácter personal acepta que un tercero utilice su información, esto se hace de maneras escrita.

EVENTO: Es un acontecimiento o cambio que no representa necesariamente un resultado negativo.

DERECHOS DE AUTOR: En la terminología jurídica, la expresión "derecho de autor" se utiliza para describir los derechos de los creadores sobre sus obras literarias y artísticas.

DISPONIBILIDAD: La disponibilidad implica que debe protegerse la información de forma tal que se pueda disponer de ella para su gestión en el tiempo y la forma requeridos por el usuario.

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

INTEGRIDAD: La integridad implica que debe salvaguardarse la totalidad y la exactitud de la información que se gestiona.

MALWARE: Software malicioso (virus, gusanos, spyware).

MEDIO REMOVIBLE: es cualquier componente extraíble de hardware que sea usado para el almacenamiento de información; los medios removibles incluyen cintas, discos duros removibles, CDs, DVDs y unidades de almacenamiento USB, entre otras.

RIESGO: efecto de la incertidumbre sobre los objetivos (ISO 31000:2012).

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

VIRUS: Programa malicioso que puede incorporarse por sí mismo en un archivo u otro programa, e infectar una computadora sin el conocimiento del usuario. Para transmitirse de un equipo a otro no infectado, requiere de una acción del usuario.

VULNERABILIDAD: Debilidad en un activo que lo hace susceptible de ser atacado.

3. NORMATIVIDAD

Este informe tiene como referencia normativa los siguientes elementos:

TIPO:	NÚMERO	NOMBRE:
Ley	1273 de 2009	De la protección de la información y de los datos
Ley	1581 de 2012	De la protección de datos personales.
Ley	1341. 30 de julio 2009	Principios y conceptos sobre la sociedad de la Información y la organización de las Tecnologías de la Información y las comunicaciones (TICS)
Otros	NTC ISO 27001:2013	Requisitos para el establecimiento, implementación, mantenimiento y mejora continua un sistema de gestión de seguridad de la información

Tabla 1 Normatividad

4. MARCO TEORICO

Para la realización del presente informe el mayor insumo y guía de trabajo es la norma ISO 27001 que brinda un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información (SGSI). La adopción de un SGSI es una decisión estratégica para una organización. El diseño e implementación del SGSI de una organización están influenciados por las necesidades y objetivos, los requisitos de seguridad, los procesos empleados y el tamaño y estructura de la organización. Se espera que estos aspectos y sus sistemas de apoyo cambien con el tiempo. Se espera que la implementación de un SGSI se ajuste de acuerdo con las necesidades de la organización, por ejemplo, una situación simple requiere una solución de SGSI simple.

Esta norma promueve la adopción de un enfoque basado en procesos, para establecer, implementar, operar, hacer seguimiento, mantener y mejorar el SGSI de una organización. Para funcionar eficazmente, una organización debe identificar y gestionar muchas actividades. Se puede considerar como un proceso cualquier actividad que use recursos y cuya gestión permita la transformación de entradas en salidas. Con frecuencia, el resultado de un proceso constituye directamente la entrada del proceso siguiente. La aplicación de un sistema de procesos dentro de una organización, junto con la identificación e interacciones entre estos procesos, y su gestión, se puede denominar como un “enfoque basado en procesos”. El enfoque basado en procesos para la gestión de la seguridad de la información, presentado en esta norma, estimula a sus usuarios a hacer énfasis en la importancia de:

a) comprender los requisitos de seguridad de la información del negocio, y la necesidad de establecer la política y objetivos en relación con la seguridad de la información;

b) implementar y operar controles para manejar los riesgos de seguridad de la información de una organización en el contexto de los riesgos globales del negocio de la organización;

c) el seguimiento y revisión del desempeño y eficacia del SGSI, y

d) la mejora continua basada en la medición de objetivos.

Esta norma adopta el modelo de procesos “Planificar-Hacer-Verificar-Actuar” (PHVA), que se aplica para estructurar todos los procesos del SGSI.

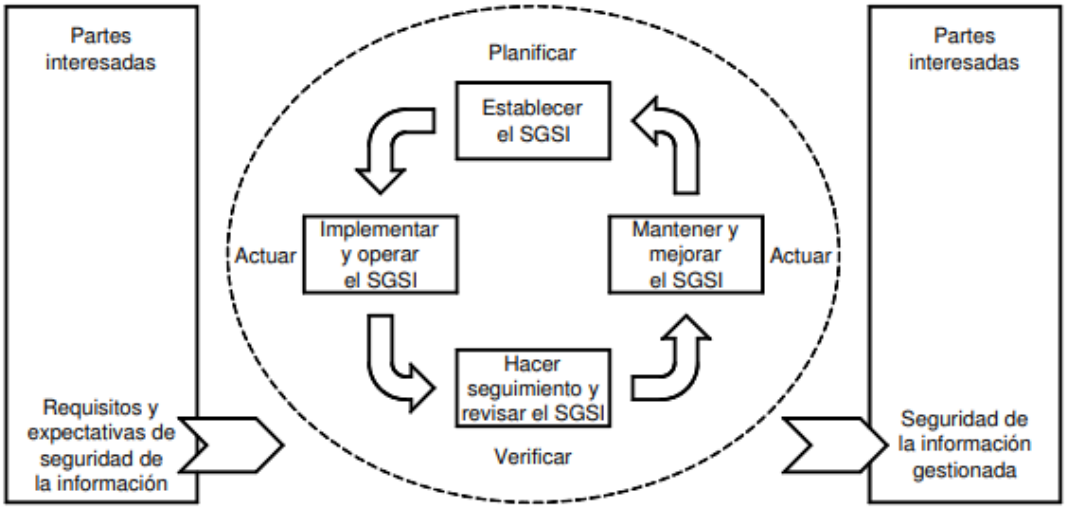


Ilustración 1 Modelo PHVA aplicado a los procesos de SGSI

5. INFORMACION DE LA INSTITUCION

SALUDVIDA EPS entidad prestadora de salud con cobertura en 22 Departamentos y 500 municipios, con más de 1.800 IPS y Clínicas de todos los niveles de complejidad para la atención de la salud de Colombianos; caracterizada por su actual modelo de salud enfocado a la promoción y prevención y reconocida como una de las 15 EPS con mejor reputación en Colombia; además de su excelente servicio y gestión en temas de salud busca caracterizarse por su compromiso frente a los temas de seguridad de la información por lo que cuenta con un área dedicada exclusivamente a esta, ubicada en la ciudad de Bogotá, ubicada en la Calle 40a # 13-06, esta sede es netamente administrativa y es el corazón de la compañía, pues desde allí se controla y monitorea tanto la seguridad de la información, como la área financiera, recursos humanos, gerencia y áreas de tecnologías y comunicaciones, siendo de gran importancia la implementación de un sistema de seguridad que garantice la confidencialidad, integridad y disponibilidad de la información.

- **Misión:** Con nuestros colaboradores, construimos un modelo de atención y servicio en salud integral, continuo y efectivo, basado en el conocimiento de nuestros afiliados y sus familias, buscando alianzas con individuos, comunidades y prestadores; para así asegurar nuestra permanencia
- **Visión**: Seremos reconocidos por la mejor experiencia de atención y servicio en salud para con nuestros afiliados y sus familias, generando valor para los grupos de interés.
- **Objetivo**: Superar los desafíos para salvaguardar la sostenibilidad de nuestra organización. Nuestros esfuerzos deben estar enfocados hacia el éxito de la implementación del Plan de Reorganización Institucional, que contiene la implementación exitosa del Modelo Integral Incluyente, la aprobación del plan de

viabilidad financiera y régimen de reservas técnicas y la mejora en el desempeño de los indicadores clave de la compañía. Este Objetivo se desarrolla a través del plan "Enfocados al Éxito"

Ilustración 2 https://www.saludvidaeps.com/index.php/ranking-eps-colombia

Jefe Inmediato: Rubén Alexander Rico

Cargo: Director Senior de Seguridad de la Información.

Correo Electrónico: rubenrico@saludvidaeps.com

6. DEFINICIÓN Y ALCANCE

Un sistema de gestión de seguridad de la información (SGSI) es para una organización el diseño, implantación, mantenimiento y mejora de un conjunto de procesos documentados y conocidos por toda la organización que se utiliza para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y mejora continua.

Para la planeación, implementación, verificación y mejora de un sistema de gestión de seguridad de la información (SGSI), se cuenta con una de las normas más importantes en la actualidad que es la ISO/IEC 27001 que establece las guías, procedimientos y procesos para gestionar de manera apropiada el sistema de gestión de seguridad de la información (SGSI), en ella se encuentran los anexos que son un marco de referencia para selección de controles dentro de este proceso, siendo una norma certificable que posibilita el mejoramiento continuo de la misma.

El presente proyecto de grado aprobado por el Comité Curricular del Programa Ingeniería de Sistemas inicia desde el análisis y evaluación de la seguridad de la información de SALUDVIDA EPS nivel central hasta el diseño de SGSI basado en la normas ISO/IEC 27001 en su fase de planeación.

7. JUSTIFICACION

Para SALUDVIDA EPS la información es uno de los activos más importantes con lo que cuenta la empresa, por lo cual diariamente la compañía se esfuerza por garantizar la confidencialidad, integridad y disponibilidad de la información contando con un área dedicada exclusivamente a este fin. Adicionalmente SALUDVIDA EPS tiene como objetivo certificarse en la norma ISO/IEC 27001, por lo cual, el propósito fundamental de la pasantía es el de apoyar y ser parte de este proceso, diseñando un sistema de gestión de seguridad de la información como principal insumo que garantice el cumplimiento de esta meta logrando así mismo el posicionamiento de la empresa a nivel nacional en este aspecto.

8. METODOLOGIA

Con el fin de alcanzar los objetivos propuestos, se realizará un análisis de los riesgos y vulnerabilidades frente a la seguridad de la información en la empresa SALUDVIDA EPS; por medio de un proyecto aplicado que contiene una propuesta de diseño de un sistema de gestión de la seguridad de la información, teniendo como base la norma ISO/IEC 27001 en su fase de planeación con sus controles y requerimientos establecidos.

9. ACCIONES DESARROLLADAS DE ACUERDO AL PLAN DE TRABAJO

ACCIONES DESARROLLADAS PRIMER CORTE	
18 de junio al 20 de junio (Alcance y metodología)	En el mes de Julio se realiza un estudio de manera analítica a la norma ISO/ 27001 con especial atención a la fase de planeación y al Anexo A, realizando mapas mentales que faciliten la comprensión de la estructura general de la norma. Así mismo se define el alcance y la metodología a utilizar del presente informe.
21 de junio al 03 de julio (Políticas de seguridad de la información)	Se inicia una evaluación de las políticas de seguridad de la información con las que actualmente cuenta SALUDVIDA EPS. Estas políticas se comparan con la normatividad vigente en busca de falencias. En éste análisis se encuentra que frente a la norma ISO/IEC 27001 se cumple con los ítems obligatorios; sin embargo en miras al mejoramiento se evidencia que no está presente la política BYOD (Dispositivos móviles no corporativos), que sin una supervisión adecuada por parte del área de seguridad de la información, podría ser una brecha de seguridad. Por otra parte se complementan las políticas de seguridad de los recursos humanos agregando la Política durante el cumplimiento de funciones, desvinculación, licencias y vacaciones o cambio de labores, que nos indican como proceder en estos casos. (*Cabe aclarar que las políticas expuestas en el presente informe no son las mismas de SALIDVIDA EPS, pues esta información no es publica y solo puede ser presentada a los funcionarios de dicha entidad*.)
04 de julio al 19 de julio (Inventario de activos de la información)	Teniendo una políticas claras frente a la seguridad de la información se procede a investigas sobre los activos de la información esenciales para el correcto funcionamiento de la compañía, aunque no se tiene acceso a todos y cada uno de ellos, se realiza una investigación donde se pueden definir los activos de información esenciales para una EPS. Como valor agregado para el sistema de gestión de seguridad de la información se diseña un plan de continuidad de negocio de Salud Vida EPS, que también es un documento requerido para el sistema de gestión de seguridad de la información.

Tabla 2 Acciones realizadas primer corte

Al culminar el primer corte se estima que el informe se encuentra en un 56% de 100%.

ACCIONES DESARROLLADAS SEGUNDO CORTE	
23 de julio al 08 de agosto (Realizar un análisis de los riesgos y vulnerabilidades frente a la seguridad de la información.)	Con la lista de activos de la información, se efectúa una valoración cualitativa, la información de la tabla es adquirida por medio de observación y preguntas al personal del área encargada, se determinan las amenazas y vulnerabilidades que podrían afectar al activo de información indicando la probabilidad de posible ocurrencia para finalmente dar una valoración y así determinar su importancia.
09 de agosto al 18 de agosto	Se realiza una comparación de los controles sugeridos en el anexo A de la norma ISO/IEC 27001 versus los implementados por la empresa,

(Revisar los controles ya existentes de seguridad de la información.)	analizando las posibles mejoras a realizar y minimizando al máximo posibles riesgos a la seguridad de la información.

Tabla 3 Acciones realizadas segundo corte

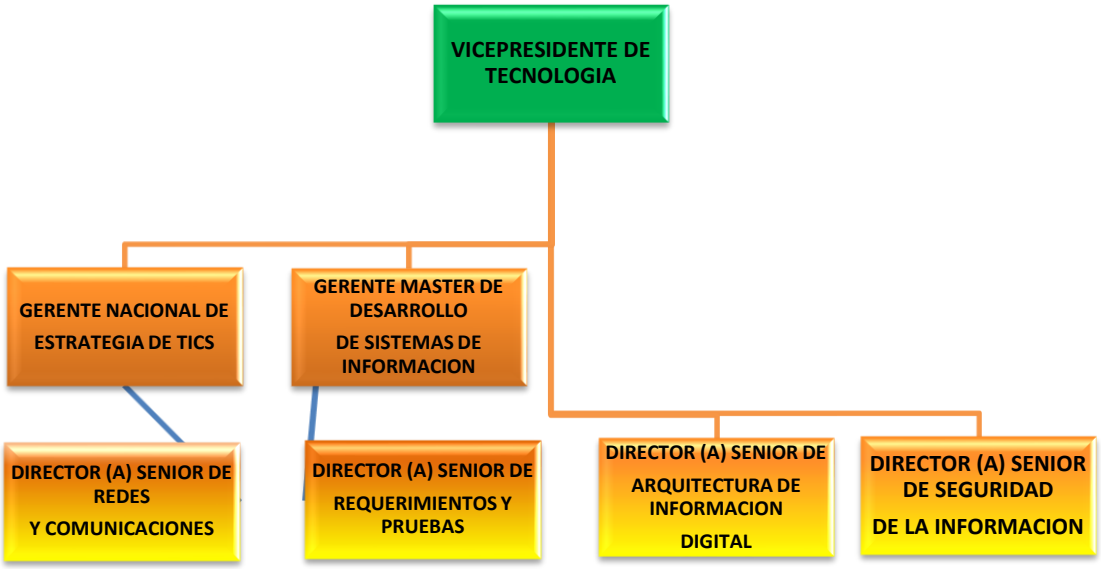
Al culminar en el segundo corte se estima que el informe se encuentra en un 84% de 100%

ACCIONES DESARROLLADAS TERCER CORTE	
22 de agosto al 22 de Septiembre	Análisis de información obtenida, obtención de resultados y afinamiento de informe, realización de presentación para socialización final, preparación para la exposición de plan de trabajo.

Al culminar las horas establecidas en el plan de trabajo el informe esta l 100%

10. DISEÑO DE GESTION DE SEGURIDAD DE LA INFORMACION

Para el diseño, establecimiento, monitoreo y mejora del sistema de gestión de la seguridad de la información es necesario es indispensable el compromiso por parte de la presidencia, en el caso particular de SALUDVIDA EPS, la presidencia y vicepresidencia de tecnología son las personas que avalan los proyectos de la dirección de seguridad de la información y en este caso particular el SGSI, la dirección de tecnologías se compone de la siguiente manera:



ALCANCE: La gestión de seguridad de la información busca establecer y mantener procedimientos, controles y políticas para conservar la confidencialidad, integridad y disponibilidad de la información de los diferentes sistemas con los que cuenta la compañía.

El sistema de gestión de la seguridad de la información será aplicado a los activos de la información de la compañía incluyendo sus las plataformas tecnológicas y sus procesos.

Dentro del alcance del SGSI están:

- Los activos de información identificados y clasificados en este informe.
- Los servidores donde se alojan dichos activos de información.
- Las oficinas de SALUDVIDA EPS.
- Sus funcionarios y contratistas.

OBJETIVO: El Sistema de Gestión de Seguridad de la Información (SGSI), tiene como objetivo general aplicar los estándares de seguridad de la información contemplados en la norma ISO 27001 a todos los activos de la información de SALUDVIDA EPS, para garantizar confiabilidad, integridad y disponibilidad de la información.

10.1 POLITICAS DE SEGURIDAD DE LA INFORMACION

10.2 OBJETIVO

Garantizar la confidencialidad, integridad y disponibilidad de los activos de información, estableciendo políticas que deben ser cumplidas por todos los empleados, contratistas y terceros en la empresa SALUD VIDA EPS.

10.3 ALCANCE

Las políticas de seguridad de la información deben ser cumplidas por toda la organización incluyendo directivos, funcionarios, proveedores y terceros que laboren o tengan algún vínculo comercial con SALUDVIDA EPS y que tengan acceso a información a través de los documentos, equipos de cómputo, infraestructura tecnológica y canales de comunicación de la Institución en busca de garantizar la confidencialidad, integridad y disponibilidad de la información.

10.4 POLITICA GLOBAL DE SEGURIDAD DE LA INFORMACION:

Los funcionarios, aprendices, proveedores y todos aquellos que tengan responsabilidades sobre los activos de la información de SALUDVIDA EPS, deben adoptar los lineamientos contenidos en el presente documento, con el fin de mantener la confidencialidad, la integridad y asegurar la disponibilidad de la información.

Se establecen políticas de seguridad de la información las cuales se fundamentan en los dominios y objetivos de control de la norma internacional ISO/IEC 27001:2014.

10.5 POLITICA DE DISPOSITIVOS MOVILES

Se suministran condiciones para el manejo de dispositivos móviles como lo son teléfonos, computadores portátiles, tabletas, etc. El objetivo es que tanto los funcionarios de SALUDVIDA EPS como los visitantes, proveedores utilicen estos dispositivos de manera responsable.

10.5.1 NORMAS PARA USO DE DISPOSITIVOS MOVILES

- La dirección debe establecer un método de bloqueo para los dispositivos móviles institucionales que serán entregados a los usuarios.
- Se deben configurar los dispositivos móviles institucionales para que durante un tiempo de inactividad establecido pasen automáticamente a modo de suspensión y se active el bloqueo de la pantalla el cual requerirá un método de desbloqueo configurado.
- El personal autorizado debe configurar la opción de borrado remoto de información en los dispositivos móviles institucionales, con el fin de eliminar los datos de dichos dispositivos y restaurarlos a los valores de fábrica, de forma

remota, evitando así divulgación no autorizada de información en caso de pérdida o hurto.

- Los dispositivos móviles institucionales deben tener una copia de seguridad actualizada.
- Los dispositivos móviles institucionales y de funcionarios que tengan autorización de conectarse a la red, tiene que tener instalado un antivirus.
- Se debe activar los códigos de seguridad de la tarjeta SIM para los dispositivos móviles institucionales antes de asignarlos a los usuarios y almacenar estos códigos en un lugar seguro.
- Los funcionarios no deben modificar las configuraciones de seguridad de los dispositivos móviles institucionales bajo su responsabilidad, ni desinstalar el software administrado con ellos al momento de su entrega.

10.6 POLITICA DE SEGURIDAD BYOD

Se definen las normas para el uso de BOYD que deben cumplir los colaboradores y contratistas de SALUDVIDA E.P.S con el fin de especificar las responsabilidades y las normas que se deben llevar a cabo para garantizar la seguridad de la información.

10.6.1 NORMAS PARA LA APLICACIÓN DE BOYD

- Los dispositivos aprobados deben estar en modo silencioso mientras se encuentre en la organización.
- Está prohibido el uso de redes inalámbricas externas no corporativas salvo 3G/4G.

- Se debe configurar el bloqueo automático del dispositivo tras un periodo de inactividad.
- Debe desactivar el teléfono a la búsqueda de redes wifi y de dispositivos vía Bluetooth cuando no sea necesario.
- Los dispositivos deben estar protegidos con contraseña.
- Se debe reportar inmediatamente, si identifica cualquier comportamiento anómalo en el dispositivo asociado a malware.
- En caso de necesitar acceso red WIFI, debe conectarse a la red de invitados de SALUDVIDA EPS.

10.7 POLITICAS DE SEGURIDAD DE RECURSOS HUMANOS

10.7.1 POLÍTICA RELACIONADA CON LA VINCULACIÓN DE FUNCIONARIOS

Salud Vida E.P.S reconoce la importancia que tiene el factor humano para el cumplimiento de sus objetivos misionales, garantizará que la vinculación de nuevos funcionarios se realizará siguiendo un proceso formal de selección, acorde con la legislación vigente, el cual estará orientado a las funciones y roles que deben desempeñar los funcionarios en sus cargos.

10.7.2 NORMAS RELACIONADAS CON LA VINCULACIÓN DE FUNCIONARIOS

- El área de Talento Humano debe realizar las verificaciones necesarias para confirmar la veracidad de la información suministrada por el personal candidato a ocupar un cargo en Salud Vida E.P.S, antes de su vinculación definitiva.

- El área de Talento Humano debe certificar que los funcionarios firmen un acuerdo y/o Cláusula de Confidencialidad y un documento de Aceptación de Políticas de Seguridad de la Información; estos documentos deben ser anexados a los demás documentos relacionados con la ocupación del cargo.
- El personal provisto por terceras partes que realicen labores en Salud Vida E.P.S deben firmar un Acuerdo y/o Cláusula de Confidencialidad y un documento de Aceptación de Políticas de Seguridad de la Información, antes de que se les otorgue acceso a las instalaciones y a la plataforma tecnológica.
- Todos los nuevos funcionarios de Salud Vida E.P.S pasaran por un periodo de inducción a las políticas, procedimientos y estándares de seguridad de la información.

10.7.3 POLITICAS DE SEGURIDAD DURANTE EL CUMPLIMIENTO DE FUNCIONES

Toda información de SALUD VIDA EPS que el colaborador, contratista o tercero pueda conocer durante el desarrollo de alguna actividad asociada a la entidad, así como la documentación suministrada, se considera confidencial y no podrá ser divulgada ni utilizada para efectos diferentes a los establecidos de manera inicial. El incumplimiento de esta obligación hará responsable al colaborador, contratista o tercero por los perjuicios que se causen directa y/o indirectamente a la compañía y conllevará a todas las implicaciones de carácter civil y penal correspondientes contra el colaborador, contratista o tercero.

10.7.4 NORMAS DE SEGURIDAD DURANTE EL CUMPLIMIENTO DE FUNCIONES

- Es el deber de cada funcionario estudiar y cumplir las políticas de seguridad de la información, asistir a charlas o entrenamientos en materias de seguridad.
- Es obligación de todo funcionario el informar las vulnerabilidades detectadas y violaciones de seguridad de la información al superior directo.
- Ningún funcionario puede violar los sistemas computacionales y redes de cualquier organización o individuo, ya sea dentro o fuera del horario de trabajo con recursos de Salud Vida E.PS

10.7.5 POLÍTICA DE DESVINCULACIÓN, LICENCIAS, VACACIONES O CAMBIO DE LABORES DE LOS FUNCIONARIOS Y PERSONAL PROVISTO POR TERCEROS

Salud Vida E.P.S asegurará que sus funcionarios y el personal provisto por terceros serán desvinculados o reasignados para la ejecución de nuevas labores de una forma ordenada, controlada y segura.

10.7.6 NORMAS PARA LA DESVINCULACIÓN, LICENCIAS, VACACIONES O CAMBIOS DE LABORES DE LOS FUNCIONARIOS Y PERSONAL PROVISTO POR TERCEROS

- El Grupo de Talento Humano debe realizar el proceso de desvinculación, licencias, vacaciones o cambio de labores de los funcionarios, llevando a cabo los procedimientos y ejecutando los controles establecidos para tal fin.
- Cada Gerente, vicepresidente, director o Jefe de Oficina debe monitorear y reportar de manera inmediata la desvinculación o cambio de labores de los funcionarios o personal

provistos por terceras partes a la mesa de servicio junto con recursos humanos y debe solicitar la inhabilitación de usuario.

10.8 POLITICAS DE TELETRABAJO

En SALUDVIDA EPS, el teletrabajo es una alternativa por lo que el acceso a la red corporativa se realiza de acuerdo al rol que el teletrabajo ejerce, se busca establecer condiciones para teletrabajo que deben cumplir los funcionarios y contratistas de Salud Vida E.P.S con el fin de determinar las responsabilidades que deben cumplir.

10.8.1 NORMAS PARA TELETRABAJO

- Los teletrabajadores deben asistir a la compañía en un cronograma ya definido y aceptado con anticipación.
- Los teltrabajadores no deben realizar configuraciones en el equipo asignado por la compañía, así como tampoco debe alterar el software con el que se le fue entregado.
- El equipo de cómputo asignado al teletrabajador no debe ser utilizado para fines personales.

10.9 POLITICAS DE RESPONSABILIDAD Y USOS ACEPTABLE DE ACTIVOS

Para SALUDVIDA EPS como propietario de la información física, así como de la información generada, procesada, almacenada y transmitida en sus plataformas tecnológicas, establecerá responsabilidad a los funcionarios sobre sus activos de información institucional, asegurando el cumplimiento de las políticas que regulan el uso adecuado de las mismas. La información, los sistemas, archivos físicos, los servicios y los equipos de propiedad del SALUDVIDA EPS, son activos de la organización y se

suministran a los funcionarios y terceros autorizados, para cumplir con los propósitos institucionales.

10.9.1 NORMAS DE RESPONSABILIDAD POR LOS ACTIVOS

- Se debe llevar un registro de los activos que posee cada funcionario, acogiendo las indicaciones de las guías de clasificación de la información; también se debe mantener actualizado el inventario de sus activos de información.
- Es necesario adoptar medidas que garanticen la seguridad de dichos activos.
- Solo el personal autorizado puede instalar, eliminar o cambiar componentes de la plataforma tecnológica de la institución.
- La Dirección de Tecnología junto con la mesa de servicio es responsable de preparar las estaciones de trabajo fijas o portátiles de los funcionarios y de hacer entrega de las mismas.
- Es necesario realizar análisis de Riesgos periódicamente sobre los procesos de SALUDVIDA EPS.
- Cada uno de los funcionarios y terceros que tengan acceso a activos de SALUDVIDA EPS deben tener claridad y utilizarlos de forma ética y en cumplimiento de las leyes y reglamentos vigentes.
- Los equipos de cómputo de SALUDVIDA EPS deben ser utilizados única y exclusivamente para fines laborales y esta prohibido el uso para propósitos personales.
- Los funcionarios no deben utilizar software no autorizado o de su propiedad en los equipos de cómputo de SALUDVIDA EPS

- Todas las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos son asignados a un responsable, por lo cual es su compromiso hacer uso adecuado y eficiente de dichos recursos.
- En el momento de desvinculación o cambio de labores, los funcionarios de SALUDVIDA EPS deben realizar la entrega de su puesto de trabajo, así mismo, deben encontrarse a paz y salvo con la entrega de los recursos tecnológicos y otros activos de información suministrados en el momento de su vinculación.

10.10 POLITICA DE CLASIFICION DE LA INFORMACION

Para determinar las medidas de seguridad a cada activo de información se debe realizar un inventario y clasificarlo, de acuerdo con el impacto que ocasionaría su difusión, alteración, acceso no autorizado, destrucción o perdida, aplicando para ello criterios de confidencialidad, integridad y disponibilidad.

10.10.1 NORMAS DE CLASIFICACION DE LA INFORMACION

- El director de Seguridad de la Información debe recomendar los niveles de clasificación de la información para que sean aprobados por la Junta Directiva.
- La vicepresidencia de tecnologías y comunicación debe definir los niveles de clasificación de la información para el SALUDVIDA EPS y, posteriormente generar la guía de clasificación de la Información.
- La dirección de seguridad de la información debe socializar y divulgar la guía de clasificación de la Información a los funcionarios de SALUDVIDA EPS.

- La Dirección de seguridad de la información debe proveer los métodos de cifrado de la información, así como debe administrar el software o herramienta utilizado para tal fin.
- La Dirección de Tecnología debe efectuar la eliminación segura de la información, a través de los mecanismos necesarios en la plataforma tecnológica, ya sea cuando son dados de baja o cambian de usuario.
- el aplicativo de nóminas es confidencial y sólo tendrán acceso a él ciertos empleados del departamento de personal para los cuales habilitaremos permisos.
- Se deben realizar de manera periódica auditorías de seguridad que certifiquen que se aplican los tratamientos estipulados para proteger la información.
- La información digital y física de SALUDVIDA EPS debe tener un periodo de almacenamiento que puede ser dictaminado por requerimientos legales o misionales; este período debe ser determinado documentalmente y cuando se cumpla el periodo de expiración, toda la información debe ser eliminada adecuadamente.
- La información que se encuentra en documentos físicos debe ser protegida, a través de controles de acceso físico y las condiciones adecuadas de almacenamiento y resguardo.

10.11 POLITICA MANEJO DE MEDIOS DE ALMACENAMIENTO

El uso de periféricos y medios de almacenamiento en los recursos de la plataforma tecnológica de SALUDVIDA EPS será reglamentado por la Vicepresidencia de Tecnología, teniendo en cuenta las labores realizadas por los funcionarios y su necesidad de uso.

10.11.1 NORMAS DE MANEJO DE MEDIOS DE ALMACENAMIENTO

- La Dirección de Tecnología y el área de seguridad de la información deben establecer las condiciones de uso de periféricos y medios de almacenamiento en la plataforma tecnológica de SALUDVIDA EPS.
- La Dirección de Tecnología y el área de seguridad de la información deben generar y aplicar lineamientos para la disposición segura de los medios de almacenamiento del SALUDVIDA EPS, ya sea cuando son dados de baja o re-asignados a un nuevo usuario.
- El director Senior de seguridad de la información debe autorizar el uso de periféricos o medios de almacenamiento en la plataforma tecnológica de SALUVIDA EPS, de acuerdo con el perfil del cargo del funcionario solicitante.
- Los funcionarios de SALUDVIDA EPS y el personal provisto por terceras partes no deben modificar la configuración de periféricos y medios de almacenamiento establecidos por la Dirección de Tecnología y el área de seguridad de la información.
- Los funcionarios y personal provisto por terceras partes son responsables por la protección de los medios de almacenamiento institucionales asignados.
- Los funcionarios y personal provisto por terceras partes no deben utilizar medios de almacenamiento personales en la plataforma tecnológica de SALUDVIDA EPS.

10.12 POLITICA DE CONTROL DE ACCESO

SALUDVIDA EPS a fin de controlar el acceso a los sistemas de información, deberá contar con mecanismos de protección para la red, los equipos y todo medio donde se encuentren activos de información, así como la implementación de perímetros de

seguridad, suministro de energía eléctrica, aire acondicionado, y cualquier otra área considerada crítica para la operatividad de la compañía.

10.12.1 NORMAS PARA CONTROL DE ACCESO

- Cada funcionario y personal provisto por terceros que labora en SALUDVIDA EPS, tiene que tener un usuario y contraseña personal para acceder a los equipos de cómputo y únicamente podrán realizar las tareas para las que fueron autorizados.
- Los funcionarios y personal provisto por terceras partes, antes de contar con acceso lógico por primera vez a la red de datos de SALUDVIDA EPS, deben contar con el formato de creación de cuentas de usuario debidamente autorizado y el Acuerdo de Confidencialidad firmado previamente.
- El área de seguridad de la información debe verificar periódicamente los controles de acceso para los usuarios provistos por terceras partes, con el fin de revisar que dichos usuarios tengan acceso permitido únicamente a aquellos recursos de red y servicios de la plataforma tecnológica para los que fueron autorizados.
- El área de seguridad de la información debe autorizar la creación o modificación de las cuentas de acceso a las redes o recursos de red.
- El área de seguridad de la información debe asegurar que las redes inalámbricas de SALUDVIDA EPS cuenten con métodos de autenticación que evite accesos no autorizados.

10.13 POLITICA DE CONTROLES CRIPTORAFICOS

SALUDVIDA EPS velará porque la información clasificada como reservada o restringida, será cifrada al momento de almacenarse y/o transmitirse por cualquier medio.

10.13.1NORMAS DE CONTROLES CRITOGRAFICOS

- La Dirección de Tecnología y el área de seguridad de la información deben verificar que todo sistema de información o aplicativo que requiera realizar transmisión de información reservada o restringida, cuente con mecanismos de cifrado de datos.
- La Dirección de Tecnología y el área de seguridad de la información deben almacenar y/o transmitir la información digital clasificada como reservada o restringida bajo técnicas de cifrado con el propósito de proteger su confidencialidad e integridad.
- La Dirección de Tecnología y el área de seguridad de la información deben desarrollar y establecer un procedimiento para el manejo y la administración de llaves de cifrado.
- Los desarrolladores deben asegurarse que los controles criptográficos de los sistemas construidos cumplen con los estándares establecidos por la Dirección de Tecnología.
- Los desarrolladores deben cifrar la información reservada o restringida y certificar la confiabilidad de los sistemas de almacenamiento de dicha información.
- Las contraseñas de los colaboradores de Salud Vida E.P.S se cifrarán con el fin de evitar un acceso no autorizado.

10.14 POLITICA DE GESTION DE LLAVES

El área de seguridad de la información de SALUDVIDA EPS, es la encargada de establecer los procedimientos en cuanto a cifrado y llaves que usara para garantizar la integridad, confidencialidad y disponibilidad de la información, para establecer el sistema de llaves se tiene como referencia la normatividad colombiana establecida.

10.14.1 NORMAS PARA GESTION DE LLAVES

- Cada solicitud de los funcionarios para acceso, actualización de llaves, debe ser autorizado por la gerencia de tics.
- Las personas autorizadas de gestionar las llaves, están en la obligación de velar por la conservación de manera segura de dicha información.

10.15 POLITICA DE SEGURIDAD FISICA Y DEL ENTORNO

SALUDVIDA EPS en defensa de la integridad, confidencialidad y disponibilidad de la información, establece normas de seguridad física y control de acceso que aseguren el perímetro de sus instalaciones a nivel central y controlará las amenazas físicas externas e internas y las condiciones medioambientales de sus oficinas.

10.15.1 NORMAS DE SEGURIDAD FISICA Y DEL ENTORNO

- Las solicitudes de acceso al centro de cómputo o a los centros de cableado deben ser aprobadas por funcionarios de la Dirección de Tecnología y el área de seguridad de la información.
- Se debe registrar el ingreso de los visitantes al centro de cómputo y a los centros de cableado, en una bitácora ubicada en la entrada de estos lugares.
- La Dirección de Tecnología y el área de seguridad de la información debe descontinuar o modificar de manera inmediata los privilegios de acceso físico al centro de cómputo y los centros de cableado que están bajo su custodia, en los eventos de desvinculación o cambio en las labores de un funcionario autorizado .
- Los funcionarios de SALUDVIDA EPS deben portar el carné que los identifica como tales en un lugar visible mientras se encuentren en las instalaciones del instituto; en caso

de pérdida del carné o tarjeta de acceso a las instalaciones, deben reportarlo a la mayor brevedad posible.

- Los funcionarios de SALUDVIDA EPS y el personal provisto por terceros partes no deben intentar ingresar a áreas a las cuales no tengan autorización.
- El área de redes y comunicaciones, con el acompañamiento de la Dirección de Tecnología y el área de seguridad de la información, deben verificar que el cableado se encuentra protegido con el fin de disminuir las intercepciones o daños.
- El área de redes y comunicaciones debe cerciorarse que los centros de cableado que están bajo su custodia, se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones e incendios.
- El área de redes y comunicaciones, con el acompañamiento de la Dirección de Tecnología y el área de seguridad de la información debe certificar la efectividad de los mecanismos de seguridad física y control de acceso al centro de cómputo, centros de cableado y demás áreas de procesamiento de información.
- Las directivas de tecnologías de la información deben velar porque las contraseñas de sistemas de alarma, cajas fuertes, llaves y otros mecanismos de seguridad de acceso a sus áreas solo sean utilizados por los funcionarios autorizados y, salvo situaciones de emergencia u otro tipo de eventos que por su naturaleza lo requieran, estos no sean transferidos a otros funcionarios.
- La Dirección de Tecnología de la información debe asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y apropiadamente autorizado e identificado; así mismo, se debe llevar control de la programación de los mantenimientos preventivos.

- La Dirección de Tecnología de la información debe velar porque los recursos de la plataforma tecnológica de SALUDVIDA EPS ubicados en el centro de cómputo se encuentra protegidos contra fallas o interrupciones eléctricas.
- Se tendrá un registro de todos los visitantes el cual incluirá la hora de entrada de salida y el lugar a donde se dirige.

10.16 POLITICA DE SEGURIDAD Y PROTECCION DE LOS EQUIPOS

Los funcionarios y el personal provisto por terceros de SALUDVIDA EPS son responsables de los equipos que manejan y les sean entregados para su uso en cumplimiento de sus funciones, objetos contractuales o actividades y deberán garantizar su custodia, integridad, buen uso, para evitar pérdidas, daño o deterioro injustificado.

10.16.1 NORMAS DE SEGURIDAD Y PROTECCION DE EQUIPOS

- La Dirección de Tecnología debe proveer los mecanismos y estrategias necesarios para proteger la confidencialidad, integridad y disponibilidad de los recursos tecnológicos, dentro y fuera de las instalaciones de SALUDVIDA EPS.
- SALUDVIDA EPS garantiza que a todos sus equipos se les realizan mantenimientos preventivos y correctivos de manera frecuente.
- El área de Tecnologías de la información bebe propender porque las áreas de carga y descarga de equipos de cómputo se encuentren aisladas del centro de cómputo y otras áreas de procesamiento de información.
- La Dirección de Tecnología de la información debe generar y aplicar lineamientos para la disposición segura de los equipos de cómputo de los funcionarios del instituto, ya sea cuando son dados de baja o cambian de usuario.

- La Dirección de Tecnología es la única área autorizada para realizar movimientos y asignaciones de recursos tecnológicos; por consiguiente, se encuentra prohibida la disposición que pueda hacer cualquier funcionario de los recursos tecnológicos de SALUDVIDA EPS.
- Los funcionarios del instituto y el personal provisto por terceras partes deben bloquear sus estaciones de trabajo en el momento de abandonar su puesto de trabajo.

10.17 POLITICA DE ESCRITORIO LIMPIO Y PANTALLA LIMPIA

Cada uno de los funcionarios contratistas y terceros de SALUDVIDA EPS, debe cumplir con las políticas establecidas, administrando información física y electrónica que se encuentra su cargo, para así poder evitar el acceso a la misma por personas no autorizadas. Se debe almacenar de forma segura documentos y elementos de almacenamiento conforme los niveles de clasificación de la información ya establecida para evitar accesos no autorizados, pérdida o daño de la información en la jornada laboral o fuera de ella.

10.17.1 NORMAS DE ESCRITORIO LIMPIO Y PANTALLA LIMPIA

- Cada una de las estaciones de trabajo debe tener un computador que a su vez y por obligación debe tener un usuario y contraseña asignada el día del ingreso a la compañía.
- Los funcionarios, contratistas y terceros de SALUDVIDA EPS, que tenga dentro de sus funciones la atención al público, deberán almacenar los documentos y dispositivos de almacenamiento bajo llave y ubicar el equipo de cómputo de tal forma que se evite la visual de la información a los visitantes no autorizados.

- Durante los lapsos de tiempo en los que se dejen desatendidas las estaciones de trabajo, los funcionarios deben bloquear la sesión del usuario para evitar que terceros no autorizados accedan a la información contenida en el computador.
- La información contenida en papel que ya no sea necesaria para SALUDVIDA EPS, debe ser destruida de tal manera que sea imposible la lectura de la misma.
- Los equipos de cómputo de SALUDVIDA EPS, deben tener deshabilitados los puertos USB y en caso de ser necesarios por sus funciones deben ser autorizados por el área de seguridad de la información.
- Las estaciones de trabajo deben de estas despejadas.

10.18 POLÍTICA DE SEGURIDAD DE LAS OPERACIONES

La Dirección de Tecnología proveerá la capacidad de procesamiento requerida en los recursos tecnológicos y sistemas de información de SALUDVIDA EPS, efectuando proyecciones de crecimiento y provisiones en la plataforma tecnológica con una periodicidad de tres meses.

10.18.1 NORMAS DE SEGURIDAD DE LAS OPERACIONES

- La Dirección de Tecnología de SALUDVIDA EPS, debe efectuar, a través de sus funcionarios, la documentación y actualización de los procedimientos relacionados con la operación y administración de la plataforma tecnológica trimestralmente.
- La Dirección de Tecnología de SALUDVIDA EPS debe proporcionar a sus funcionarios manuales de configuración y operación de los sistemas operativos, firmware, servicios de red, bases de datos y sistemas de información que conforman la plataforma tecnológica, de acuerdo a sus funciones.

- El área de seguridad de la información debe emitir concepto y generar recomendaciones acerca de las soluciones de seguridad seleccionadas para la plataforma tecnológica de SALUDVIDA EPS.

10.19 POLITICAS DE CONTROL DE SOFTWARE OPERACIONAL

En SALUDVIDA EPS se llevara un control estricto del software que será instalado en la plataforma tecnológica verificando la originalidad del mismo y contara con el soporte por parte de los proveedores tanto en la instalación como en **las actualizaciones.**

10.19.1 NORMAS DE CONTROL DE SOFTWARE OPERACIONAL

- La dirección tecnológica junto con el área de seguridad de la información de SALUDVIDA EPS, debe asignar responsabilidades a los funcionarios encargados de instalación, implementación y actualización del software operacional.
- La dirección de tecnología junto con el área de seguridad de la información deben asegurarse que el software instalado en la compañía cuenten con soporte por parte del proveedor.
- La Dirección de Tecnología junto con el área de seguridad de la información debe establecer las restricciones y limitaciones para la instalación de software operativo en los equipos de cómputo del instituto.
- La Dirección de Tecnología junto con el área de seguridad de la información debe conceder accesos temporales y controlados a los proveedores para realizar las actualizaciones sobre el software operativo, así como monitorear dichas actualizaciones.

10.20 POLITICAS DE GESTIÓN DE VULNERABILIDADES

En SALUDVIDA EPS, nos preocupamos cada día por mejorar los sistemas de seguridad de la información y por ello se compromete a analizar cada una de las vulnerabilidades que se vallan encontrando en su labor diaria y mejorar en cada vulnerabilidad que represente una brecha que permita fuga de información o atente contra la disponibilidad, integridad y confidencialidad de la información.

10.20.1NORMAS DE GESTIÓN DE VULNERABILIDADES

- Todos los gerentes y directivas se reunirán cada semana en comité para realizar un análisis de vulnerabilidades que se puedan encontrar con el fin de lograr tener un plan de continencia en caso que estas vulnerabilidades se conviertan en incidentes.
- El área de seguridad de la información debe tener unos procedimientos establecidos que se deben llevar a cabo con las vulnerabilidades que se presenten.
- Se debe concientizar a los funcionarios y terceros que laboren en SALUDVIDA EPS, de informar ante cualquier vulnerabilidad de la información que les resulte importante al área de seguridad de la información.
- La Dirección de Tecnología y el área de seguridad de la información, a través del Comité semanal efectuado con los líderes del área de tecnología, deben revisar, valorar y gestionar las vulnerabilidades técnicas encontradas, apoyándose en herramientas tecnológicas para su identificación.

10.21 POLITICA COPIAS DE RESPALDO

Con esta política se busca que toda información se pueda recuperar después de un incidente y se pueda recuperar después de una falla o desastre, en busca de responder de manera rápida y

efectiva ante eventos y restablecer de manera pronta el normal funcionamiento de SALUDVIDA EPS.

10.21.1 NORMAS PARA COPIAS DE RESPALDO

- El área de tecnologías de la información y seguridad de la información deben designar personal especializado que asuma la responsabilidad de realizar backups a todos los activos de información.
- Se debe tener un inventario de activos de la información crítica y clasificarla con el fin para reanudar el negocio en caso de desastre o incidente grave.
- El sitio donde se guardan las copias de seguridad debe ser especialmente custodiado para evitar el acceso a personal no autorizado.
- Se deben haces copias de seguridad de la información crítica corporativa, la exigida por la ley y la establecida en los contratos.
- Las copias de seguridad se deben realizar todos los días.
- Las copias de seguridad se deben conservar por el tiempo que la ley lo designa.
- Se deben tener copias de seguridad de la información crítica fuera de las instalaciones resguardas con llave.
- Se deben reconocer las situaciones que serán identificadas como emergencia desastre para SALUDVIDA EPS, los procesos o las áreas y determinar cómo se debe actuar sobre las mismas.

10.22 POLITICA DE SEGURIDAD DE LAS COMUNICACIONES

10.22.1 POLÍTICA DE GESTIÓN DE LA SEGURIDAD DE LAS REDES

SALUDVIDA EPS gestionara los mecanismos de control que garanticen los accesos a redes de datos institucionales e que impidan el acceso a personal no autorizado**.**

- El área de Tecnología, redes y comunicaciones garantiza la disponibilidad de los recursos tecnológicos y servicios d red los funcionarios y terceros de SALUDVIA EPS**.**
- Se debe garantizar la disponibilidad, integridad y confidencialidad de los datos que pasan por las redes de SALUDVIDA EPS**.**
- El área de seguridad de la información es la encargada de monitorear el funcionamiento de red que está a cargo de terceros, para garantizar su buena gestión.
- Las cuentas que utilizan los proveedores para mantenimiento remoto, se activan únicamente durante el periodo de tiempo necesario**.**
- No deben de existir puntos de red habilitados en lugares de acceso público o puestos de trabajo que no estén siendo utilizados.

10.22.2 POLÍTICA DE USO DEL CORREO ELECTRONICO

SALUDVIDA EPS provee un correo electrónico corporativo, con la intención de facilitar la comunicación entre sus funcionarios y terceros, garantizando la confidencialidad, integridad y disponibilidad.

- En SALUDVIDA EPS el correo corporativo se debe utilizar única y exclusivamente para cuestiones laborales.

- El área de seguridad de información debe generar y divulgar un procedimiento para la administración de cuentas de correo electrónico.
- La cuenta de correo corporativo dado en el momento del ingreso es única e intransferible.
- Toda la información contenida en el correo corporativo es de propiedad de SALUDVIDA EPS.
- Está totalmente prohibido el envío de archivos que contengan extensiones ejecutables.
- En el correo corporativo de SALUDVIDA EPS, está prohibido él envió de propaganda, cadenas y todo material distinto a l empresarial.

10.22.3POLÍTICA DE USO ADECUADO DE INTERNET

SALUDVIDA EPS, proporciona todos los recursos a sus funcionarios para el buen desempeño de sus labores, por lo que garantiza que tengan acceso a internet pero única y exclusivamente para cuestiones laborales.

- El área de Seguridad de la información, monitorea frecuentemente el contenido que frecuentan los funcionarios de SALUDVIDA EPS.
- El área de seguridad de la información concientiza a los funcionarios de salud vida sobre las precauciones que deben tener en la navegación.
- Esta totalmente prohibido la descarga de software no autorizado.
- No está permitido el acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral.
- El acceso a redes sociales en las instalaciones de SALUDVIDA EPS, está prohibido.

10.23 POLITICA DE TRANSFERENCIA DE INFORMACION

Se establecen pautas de transferencia de información para proteger la seguridad de la información transferida dentro de Salud Vida E.P.S y la información transferida con otras entidades externas.

10.23.1 NORMAS DE TRANSFERENCIA DE INFORMACION

- Todo funcionario o tercero debe ser responsable en el manejo de la información y asimismo debe velar por su seguridad.
- Toda información que se requiera trasladar en un medio físico deberá estar regida bajo los estándares de empaquetado y debe ser autorizado por el área de seguridad de la información.
- Toda información que se requiera trasladar en un medio físico estará cifrada para evitar el acceso o modificación no autorizada.
- El área de seguridad de la información, establece procedimientos e implanta controles que permiten detectar y proteger la plataforma de correo electrónico contra código malicioso que pudiera ser transmitido a través de los mensajes

10.24 POLITICA DE DESARROLLO SEGURO

En SALUDVIDA EPS, se lleva un control estricto tanto en el desarrollo interno, como con los proveedores donde se exigen cumplir con los lineamientos estipulados y la metodología a utilizar.

10.24.1 NORMAS PARA EL DESARROLLO SEGURO

- Cada una de las etapas del desarrollo del software deben estar documentadas con el objetivo de generar registros de trazabilidad frente a los requerimientos, desarrollo y aceptación del software.
- Para el desarrollo y puesta de producción del software, se deben usar ambientes separados (lógica o físicamente): uno para el desarrollo, uno para las pruebas y uno final para la puesta en producción.
- Para acceder a los sistemas de información de Salud Vida E.P.S los colaboradores autorizados tendrán un usuario y contraseña que le serán asignados para su uso personal.
- Se tendrá un plan de contingencia para abordar cualquier peligro que pueda llegar a tener los servidores de las aplicaciones.
- En el desarrollo de software se debe llevar a cabo un control de versiones con los respectivos documentos de soporte, con el objeto de verificar el buen funcionamiento del software y el respectivo control de su ciclo de vida.
- Los sistemas de SALUDVIDA E.P.S protegerán la confidencialidad e integridad de información para que no sea modificada ni visualizada por personal no autorizado.
- Los cambios realizados en los sistemas de información de SALUDVIDA E.P.S se analizarán antes de la implementación para asegurar que todo funciona correctamente

10.25 POLITICA DE SEGURIDAD DE LA INFORMACION PARA LAS RELACIONES CON PROVEEDORES

La presente política busca mitigar los riesgos asociados a los sistemas de información, describiendo las responsabilidades del personal que pertenece a las empresas proveedoras de

servicios que trabajan para SALUDVIDA EPS, y que en el desarrollo de sus funciones pueda tener acceso a la información, sistemas de información o recursos con el fin de proteger la confidencialidad, integridad y disponibilidad de la información.

10.25.1NORMAS PARA LAS RELACIO0NES CON PROVEEDORES

- Las empresas proveedoras de servicios de SALUDVIDA EPS deben ser lealmente establecidas por la ley.
- Cada uno de los proveedores debe tener en su compañía política de seguridad de la información y manual de continuidad del negocio.
- Las empresas proveedoras deben firmar un acuerdo confidencialidad de la información.
- Cada uno de los funcionarios que pertenezcan a una empresa proveedora debe cumplir las políticas de seguridad de la información de SALUDVIDA EPS.

10.26 POLITICA DE GESTION DE INCIDENTES

SALUD VIDA EPS promoverá entre los funcionarios y personal provisto por terceras partes el reporte de incidentes relacionados con la seguridad de la información y sus medios de procesamiento, incluyendo cualquier tipo de medio de almacenamiento de información, como la plataforma tecnológica, los sistemas de información, los medios físicos de almacenamiento y las personas. Esta Política de Gestión de Incidentes de Seguridad de la Información será integrada a la normativa del SALUD VIDA E.P.S, incluyendo su difusión previa.

10.26.1NORMAS DE GESTION DE INCIDENTES

- El área de seguridad de la información debe establecer responsabilidades y procedimientos para asegurar una respuesta rápida, ordenada y efectiva frente a los incidentes de seguridad de la información.
- Todo funcionario o tercero que labore en SALUDVIDA está en la obligación de reportar al área de seguridad de la información cualquier incidente de seguridad que identifiquen o que reconozcan su posibilidad de materialización.
- La Dirección de Seguridad de la Información debe establecer responsabilidades y procedimientos para asegurar una respuesta rápida, ordenada y efectiva frente a los incidentes de seguridad de la información.
- La Dirección de Seguridad de la Información debe analizar los incidentes de seguridad que le son escalados y activar el procedimiento de contacto con las autoridades, cuando lo estime necesario.
- En caso de conocer la pérdida o divulgación no autorizada de información clasificada como uso interno, reservada o restringida, los funcionarios deben notificarlo a la La Dirección de Seguridad de la Información para que se registre y se le dé el trámite necesario.

10.27 POLITICA DE CONTINUIDAD DEL NEGOCIO

En SALUD VIDA contamos con un manual de continuidad de negocio que especifica cada uno de los lineamientos a seguir en caso de presentarse un incidente y reglamente un proceder antes estos acontecimientos, que tiene objetivo proteger los procesos críticos del negocio.

10.27.1 NORMAS PARA LA CONTINUIDAD DEL NEGOCIO

- En SALUDVIDA EPS, se cuenta con proveedores que garantizan tener planes de continencia en casos de incidentes.
- En SALUDVIDA EPS se programan periódicamente comités semanales en busca posibles riesgos y cómo afrontarlos en caso que se materialicen.
- En SALUDVIDAA EPS se deben realizar simulacros por lo menos 1 vez cada 6 meses.
- El Plan de Continuidad del Negocio (BCP,DRP), busca mitigar el riesgo a fallas o desastres, mediante un plan que permita la pronta recuperación de la operación.

10.28 POLITICA DE CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES

SALUDVIDA EPS es una compañía legalmente establecida por lo que cumple con todos los lineamientos exigidos por el Gobierno Nacional, preocupados especialmente por el uso software con licencia y ofrezca respaldo**.**

10.28.1 NORMAS DE CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES

- Se debe identificar toda la legislación aplicable a SALUDVIDA E.P.S.
- Está prohibido que todos los funcionarios y terceros de SALUDVIDA EPS, dupliquen software es sus estaciones de trabajo.
- Los funcionarios e SALUD VIDA EPS, deben estar conscientes de la responsabilidad y las implicaciones legales que ameriten en caso de violar la ley 1581 del 2012.

- Las áreas que procesan datos personales de beneficiarios, funcionarios, proveedores y terceras partes deben asegurar que solo las personas autorizadas puedan tener acceso a dichos datos.

11. INVENTARIO DE ACTIVOS DE LA INFORMACION

El inventario y clasificación de los Activos de Información de SALUDVIDA EPS 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 para SALUDVIDA EPS y 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 almacenado 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.

11.1 Niveles de clasificación de la información

Los activos de SALUDVIDA EPS, están debidamente clasificados en cada uno de los siguientes niveles:

Información Pública: Esta información puede ser de conocimiento público y su divulgación no representa ningún perjuicio para SALUDVIDA EPS.

Información de uso interno: Es toda información a la que tienen acceso sus funcionarios para la correcta función de sus labores, dentro de estas están las políticas, comunicados, etc.

Información confidencial: Es toda información a la que tienen acceso solo un grupo de funcionarios y no puede ser conocida por ningún otro miembro de la organización o tercero,

de ser conocida sin autorización de sus propietario, esta puede ser perjudicial y acarrearía sanciones legales a quien la divulgue.

Planilla para la identificación del inventario de información					
Nombre del activo	**Descripción**	**Área responsable del activo**	**Clasificación**	**Relevancia el activo**	**Soporte de información**
Indicadores de calidad	Monitorear la calidad de los servicios de salud para estimular la competencia entre los agentes del sector y orientar a los usuarios en el conocimiento de las características del sistema, en el ejercicio de sus derechos y deberes, para que tome decisiones informadas al momento de ejercer los derechos que contempla el Sistema General de Seguridad Social en Salud.	Gestión de calidad	Uso Interno	Importante	Digital
Políticas de SALUDVIDA EPS	Establece las políticas que deben cumplir los colaboradores, contratistas y terceros de SALUD VIDA E.P.S, esta información se encuentra contenida en un repositorio institucional.	Gestión de Calidad	Uso interno	Importante	Digital
Actas comités	Cada área de la organización tiene un archivo físico con las actas, debidamente firmadas de los comités realizados.	Directivas y Vicepresidencias	Confidencial	Importante	Físico
Informe de auditorias	Contiene toda la información relevante observada en el desarrollo de la auditoría, las conclusiones, las recomendaciones pertinentes, y los planes de acción asumidas por los auditados.	Gestión de calidad	Confidencial	Importante	Digital/ Físico
Informe capacidad instalada	La capacidad instalada de producción anual de acuerdo a factores de estructura: Recursos Físicos, Recursos Humanos, Recursos Financieros y la estructura Funcional Hospitalaria.	Gestión de Calidad	Confidencial	Importante	Digital
Portafolio de	El portafolio de servicios	Gestión de Calidad	Publica	Importante	Digital

servicios	es la presentación de la empresa. Identifica los servicios prestados acorde a los procedimientos establecidos en el POS (Plan Obligatorio de Salud)				
Informe seguimiento planes de mejoramiento	Hacer seguimiento permanente a las acciones de mejoramiento a ejecutar en los planes de mejora y actuar, es decir, que tan pronto sea detectado un problema, se identifiquen las causas y se busquen soluciones oportunas.	Gestión de calidad	Uso Interno	Importante	Digital
Autoevaluación estándares de habilitación	Ejercicio que realiza la entidad revisando las características de cada uno de los servicios que va a inscribir o habilitar, contra los estándares y criterios de la resolución 2003 de 2006, para determine si el servicio Cumple con todos y cada uno de los criterios establecidos en las normas que le aplican a sus servicios.	Gestión de calidad	Confidencial	Importante	Digital/Físico
Información y personal aspirantes a empleo	Información personal, copia de documentos importantes tales como diplomas, hoja de Vida, certificados etc.	Recursos Humanos	Confidencial	Importante	Digital/Física
Estados financieros	Consolidar la información contable de la entidad en un periodo determinado, con el fin que permita entregar información oportuna, confiable y veraz a la comunidad en general, los organismos de control y la gerencia, que contribuya a una adecuada toma de decisiones.	Administrativo y financiero	Confidencial y para entidades del gobierno	Importante	Digital/Física
Informes Financieros	Rendir a los diferentes organismos de control del estado la información financiera en las condiciones y términos requeridos por cada uno de ellos, con el fin que sirvan de base para evaluaciones del sector salud.	Administrativo y financiero	Confidencial y para entidades del gobierno	Importante	Digital/Física
Registros Contables	Registrar, ajustar consolidar información contable.	Administrativo y financiero	Confidencial y para entidades del gobierno	Importante	Digital/Física

Libros Contables	Consolidar los registros contables de la entidad de acuerdo a la norma contable sobre la preparación, generación y presentación de libros contables, los cuales servirán de soporte a las operaciones contables.	Administrativo y financiero	Confidencial y para entidades del gobierno	Importante	Digital/Física
Base de datos Proveedores	Es necesario conocer nombre, nit, cedula, del proveedor, sus sistemas de seguridad de la información, gestión de incidentes, manual continuidad del negocio, para su previa contratación	Área Jurídica y administrativa	Confidencial	Importante	Digital
Datos financieros de Muebles e Inmuebles	Al momento de realizar el inventario y entradas a almacén es necesario conocer el valor del bien para definir cómo será su proceso de baja en caso de que aplique.	Área jurídica y administrativa	Confidencial	Importante	Digital/ Fisica
Bases de datos pacientes	Las bases de datos y servidores, están manejados por proveedores, sin embargo desde el área de las TICS se lleva un seguimiento y control de las mismas.	Tecnología de la información	Confidencial	Importante	Digital
Informes	Registro documentado de los procesos	Control Interno	Confidencial	Importante	Digital/ Fisica
Planes de mejoramiento institucional	Acciones preventivas y correctivas de producto de las auditorías externas-entidades de control	Control Interno	Confidencial	Importante	Digital
Planes de mejoramiento por proceso	Acciones preventivas y correctivas de producto de las auditorías internas.	Control Interno	Uso interno	Importante	Digital/ Física
Evaluación del sistema de control interno	Registro de autocontrol en aplicativo portal SaludVida	Control Interno	Confidencial	Importante	Digital/ Física
Mapa de riesgos por proceso	Registro documentado del mapa de riegos por procesos	Control Interno	Confidencial	Importante	Digital

Tabla 4 Activos de la información

Como resultado de la tabla anterior en la que se realiza un inventario y clasificación de activos de la información se puede encontrar que el 76% la información es de tipo confidencial, seguida por difusión de uso interno con 19% y solo el 5% de la información es pública.
Todos los activos del inventario son de importancia alta y en su gran mayoría se encuentra de manera digital y física.

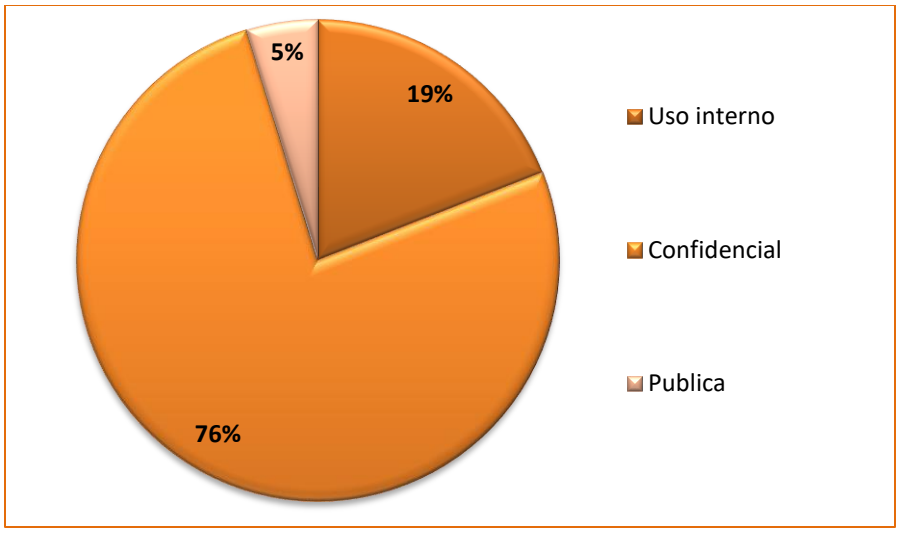


Ilustración 3 Clasificación de la información

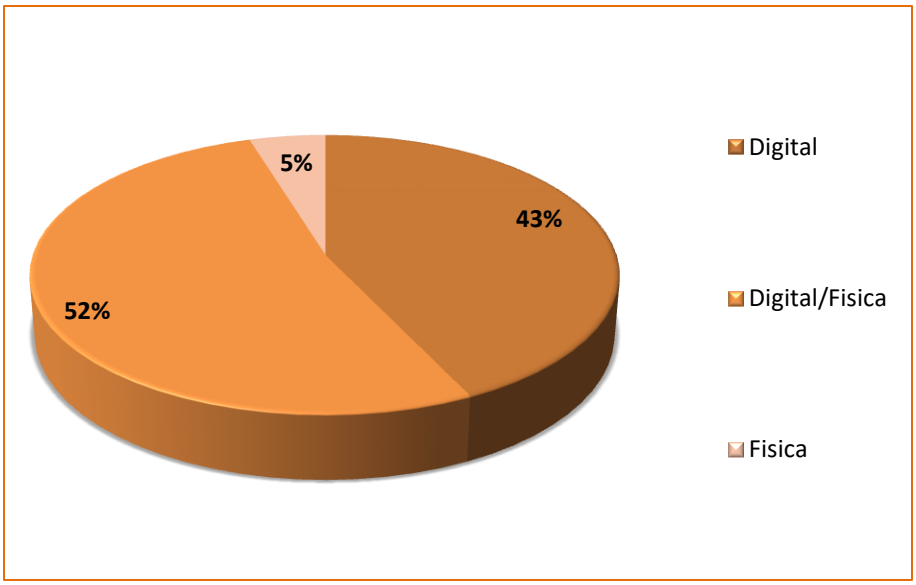


Ilustración 4 Formato de información

12. ANALISIS DE RIESGOS

12.1 ANÁLISIS Y CLASIFICACIÓN DE VULNERABILIDADES Y RIESGOS

Este análisis y clasificación de riesgos está ejecutado sobre los activos de información de SALUDVIDA EPS que ya han sido identificados con anterioridad, para posteriormente implementar los controles del anexo A, que tendrán que implementarse para mitigar los riesgos

de acuerdo a su valor para la compañía, comparando con que existen actualmente en la compañía con los que dice la norma en el anexo A.

Para el análisis se realiza una descripción cualitativa que nos lleva a concluir de manera exacta el nivel de riesgo de los activos.

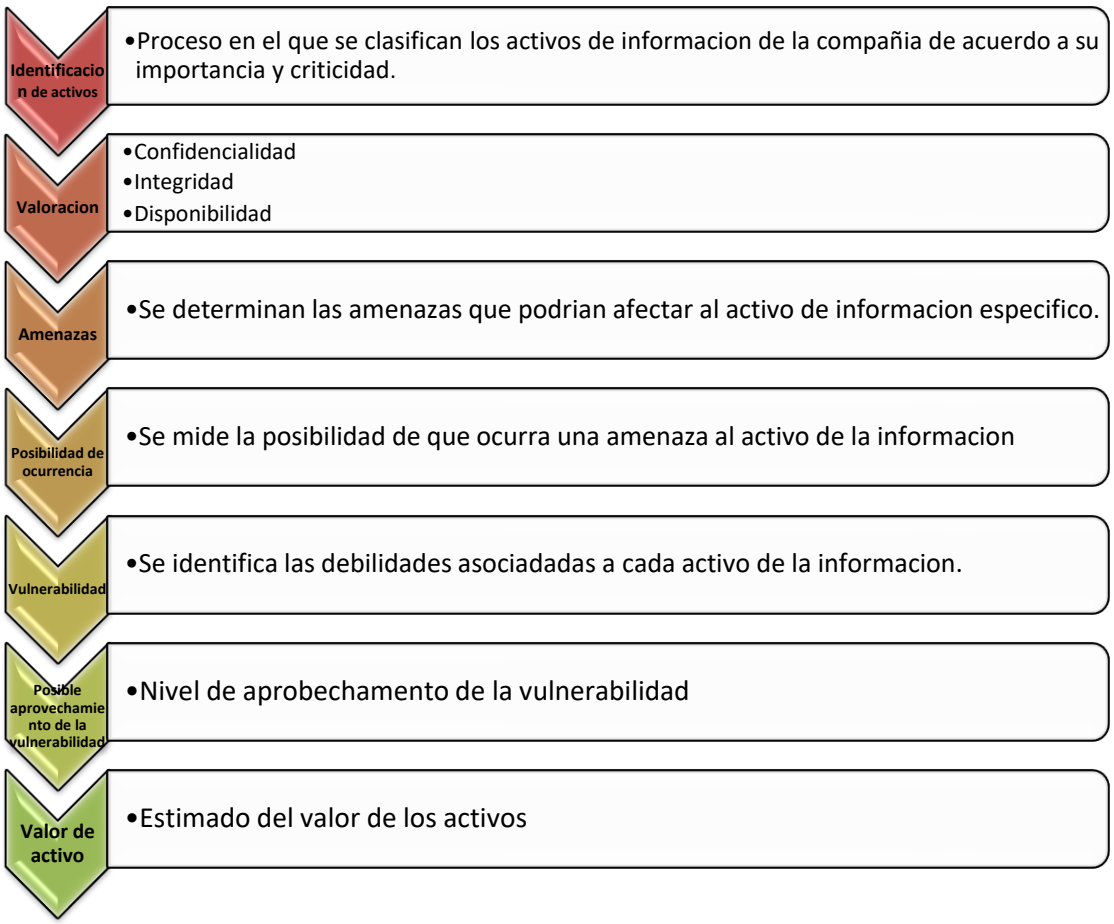


Ilustración 5 Metodologia para el analisisi y evaluacion de riesgo

Para la valoración de Amenazas y riesgos de la siguiente tabla se manejó una escala cualitativa que varía entre: ALTO, MEDIO y BAJO.

Determinados de la siguiente manera:

ALTO = A, MEDIO = M, BAJO = B

12.2 REALIZACION DE ANALISIS Y EVALUACION DE RIESGO

ACTIVO	VALORACION			AMENAZA	POSIBILIDAD DE OCURRENCIA	VULNERABILIDAD	APROVECHAMIENTO DE LA VULNERABILIDAD
	Confidencialidad	Integridad	Disponibilidad				
Indicadores de calidad	M	A	A	• Perdida • Alteración • Malware	B B M	• Error humano • Desconocimiento de rutas	M M
Actas comités	A	A	A	• Perdida • Alteración • Ilegibilidad de datos • Desastre Natural	B B M B	• Protección física no adecuada. • Falta de BackUp. • Falta de conciencia de seguridad.	M A M
Informe de auditorias	A	A	A	• Malware • Perdida • Manipulación de datos sin autorización. • Alteración • Privacidad	M B M B B	• Protección física no adecuada. • Falta de BackUp. • Falta de conciencia de seguridad • Error humano • No cerrar sesión antes de alejarse del equipo.	M M M M M
Informe capacidad instalada	A	A	A	• Manipulació	M	• No cerrar	M

				n de datos sin autorización. • Perdida • Alteración • Privacidad • Malware	B B B M	sesión antes de alejarse del equipo. • Desconocimiento de rutas • Falta de BackUp.	 M M
Portafolio de servicios	B	A	A	• Alteración • Perdida • Malware • Falsificación • Plagio	B B B B M	• Desconocimiento de rutas. • Falta de BackUp.	M B
Informe seguimiento planes de mejoramiento	M	A	A	• Manipulación de datos sin autorización. • Perdida • Alteración • Privacidad • Malware	B B B B B	• No cerrar sesión antes de alejarse del equipo. • Desconocimiento de rutas • Falta de BackUp.	M M M
Autoevaluación estándares de habilitación	A	A	A	• Malware • Perdida • Manipulación de datos sin autorización. • Alteración • Privacidad • Ilegibilidad de datos	M B M B B	• Protección física no adecuada. • Falta de BackUp. • Falta de conciencia de seguridad • Error humano • No cerrar sesión antes	M M M M M

						de alejarse del equipo.	
Información y personal de aspirantes a empleo	A	A	A	• Malware • Perdida • Manipulación de datos sin autorización. • Alteración • Privacidad • Ilegibilidad de datos	M B M B B	• Protección física no adecuada. • Falta de BackUp. • Falta de conciencia de seguridad • Error humano • No cerrar sesión antes de alejarse del equipo.	M M M M M
Estados financieros	A	A	A	• Malware • Perdida • Manipulación de datos sin autorización. • Alteración • Privacidad • Ilegibilidad de datos	M B M B B	• Protección física no adecuada. • Falta de BackUp. • Falta de conciencia de seguridad • Error humano • No cerrar sesión antes de alejarse del equipo.	M M M M M
Informes financieros	A	A	A	• Malware • Perdida	M B	• Protección física no	M

				• Manipulación de datos sin autorización. • Alteración • Privacidad • Ilegibilidad de datos	M B B	adecuada. • Falta de BackUp. • Falta de conciencia de seguridad • Error humano • No cerrar sesión antes de alejarse del equipo.	M M M M
Registros Contables	A	A	A	• Malware • Perdida • Manipulación de datos sin autorización. • Alteración • Privacidad • Ilegibilidad de datos	M B M B B	• Protección física no adecuada. • Falta de BackUp. • Falta de conciencia de seguridad • Error humano • No cerrar sesión antes de alejarse del equipo.	M M M M M
Libros Contables	A	A	A	• Perdida • Alteración • Ilegibilidad de datos • Privacidad • Desastre	B B M M B	• Protección física no adecuada. • Falta de BackUp. • Falta de	M M M

				natural		conciencia de seguridad	
Base de datos Proveedores	A	A	A	• Manipulación de datos sin autorización. • Perdida • Alteración • Privacidad • Malware	M B B B M	• No cerrar sesión antes de alejarse del equipo. • Desconocimiento de rutas • Falta de BackUp.	M M M
Datos financieros de Muebles e Inmuebles	A	A	A	• Perdida • Alteración • Ilegibilidad de datos • Privacidad • Desastre natural	B B M M B	• Protección física no adecuada. • Falta de BackUp. • Falta de conciencia de seguridad	M M M
Bases de datos pacientes	A	A	A	• Plagio • Falsificación • Alteración • Privacidad • Malware	B B B A	• Error humano. • Fuga de información.	M M
Informes	A	A	A	• Perdida • Alteración • Ilegibilidad de datos • Privacidad • Desastre natural	B B M M B	• Protección física no adecuada. • Falta de BackUp. • Falta de conciencia de seguridad	M M M
Planes de mejoramiento	A	A	A	• Plagio	B	• Error	M

institucional				• Falsificación • Alteración • Privacidad • Malware	B B A	humano. • Fuga de información.	M
Planes de mejoramiento por proceso	A	A	A	• Perdida • Alteración • Ilegibilidad de datos • Privacidad • Desastre natural	B B M M B	• Protección física no adecuada. • Falta de BackUp. • Falta de conciencia de seguridad	M M M
Evaluación del sistema de control interno	A	A	A	• Perdida • Alteración • Ilegibilidad de datos • Privacidad • Desastre natural	B B M M B	• Protección física no adecuada. • Falta de BackUp. • Falta de conciencia de seguridad	M M M
Mapa de riesgos por proceso	A	A	A	• Manipulación de datos sin autorización. • Perdida • Alteración • Privacidad • Malware	B B B B B	• No cerrar sesión antes de alejarse del equipo. •Desconocimiento de rutas • Falta de BackUp	M M M
Información CUPS	A	A	A	• Perdida • Alteración • Privacidad • Malware	B B B B	• No cerrar sesión antes de alejarse del equipo.	M

				• Manipulación de datos sin autorización.	M	•Desconocimiento de rutas • Falta de BackUp	M M
Información PQRS	A	A	A	• Perdida • Alteración • Privacidad • Malware • Manipulación de datos sin autorización.	B B B B M	• No cerrar sesión antes de alejarse del equipo. •Desconocimiento de rutas • Falta de BackUp	M M M
Base de datos funcionarios	A	A	A	• Perdida • Alteración • Ilegibilidad de datos • Privacidad • Desastre natural • Malware	B B M M B B	• Protección física no adecuada. • Falta de BackUp. • Falta de conciencia de seguridad	M M M
Software corporativo	A	A	A	• Plagio • Falsificación • Alteración • Privacidad • Malware	B B B A	• Error humano. • Fuga de información.	M M

Tabla 5 Análisis y evaluación de riesgos

En la tabla de evaluación de riesgos y vulnerabilidades se encuentra que la valoración en cuanto a confidencialidad, integridad y disponibilidad de los activos es alta se puede evidenciar que la amenaza que más se repite es la alteración de los datos con 23 repeticiones, seguida por la perdida y privacidad de la misma con 22 repeticiones, cada una con una probabilidad de ocurrencia baja.

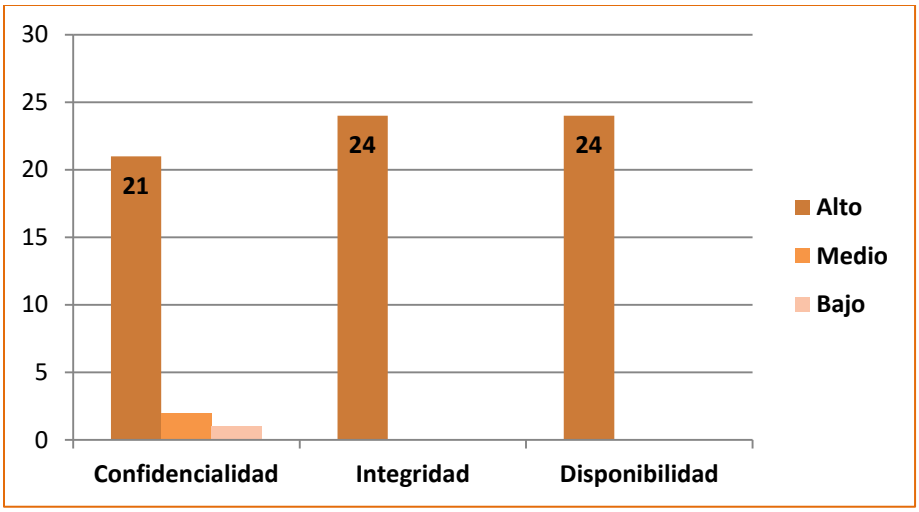


Ilustración 6 Valoración de activos.

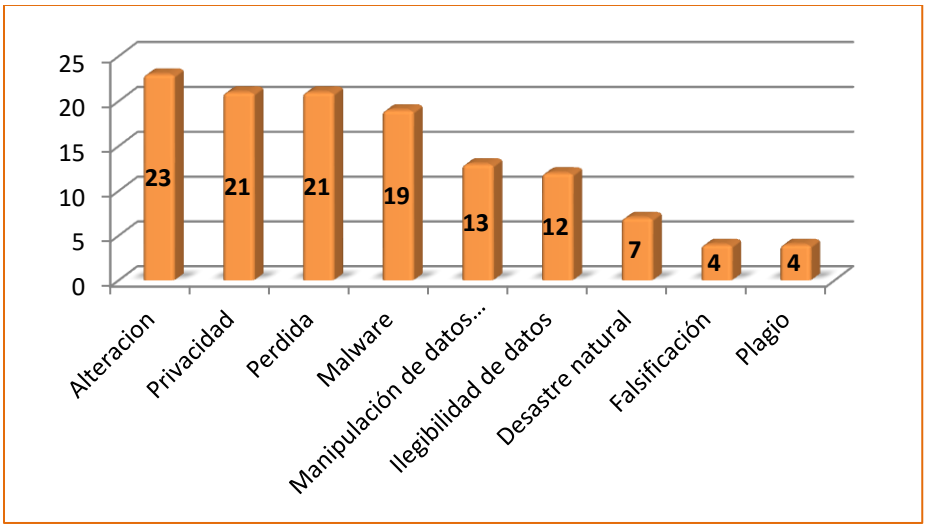


Ilustración 7 Amenazas detectadas

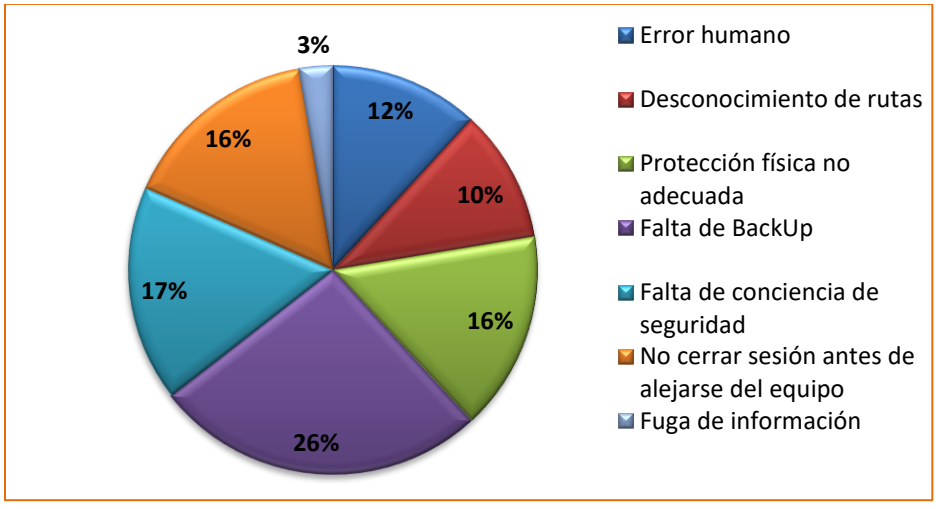


Ilustración 8 Vulnerabilidades

13. TRATAMIENTO DE RIESGOS Y CONTROLES

En SALUD VIDA EPS, los riesgo se tratan siguiendo las directrices de la norma ISO/IEC 27001 y la selección de los mismos está ajustada a las conclusiones del análisis y evaluación de riesgos antes realizado, se aplican controles para cada área de la compañía y como guía se estable el anexo A de la norma ISO/IEC 27001 donde se realiza una valoración en porcentaje de acuerdo a lo observado en el período de tiempo laborado en el área de seguridad de la información de SALUDVIDA EPS.

13.1 ALCANCE

Se definen los controles que aplican para SALUDVIDA EPS Nivel central y su propósito es mitigar los riesgos a los activos de la información

Numerales	Objetivos	Control		Control y porcentaje	Observaciones
A.5 Políticas de Seguridad de la información	A.5.1: Orientación de la dirección para la gestión de la seguridad de la información	A.5. 1.1	Políticas para la seguridad de la información	SI	SALUDVIDA EPS define un conjunto de políticas de seguridad de la información
		A.5. 1.2	Revisión de las políticas	SI	Como parte de mi trabajo en SALUDVIDA EPS hago revisión de políticas y complemento algunas y adjunto otras como: • Política de seguridad BYOD • Política durante cumplimiento defunciones. • Política de desvinculación, licencias, vacaciones o cambio de labores.
A.6 Organización de la seguridad	A.6.1: Organización interna	A.6. 1.1	Roles y responsabilidades para la seguridad de la información	SI	Asignar roles y responsabilidades para la implantación de la seguridad de la información.

de la información		A.6.1.2	Separación de deberes	SI	Se debe tener un control por cada área para restringir acceso a los activos de la organización
		A.6.1.3	Contacto con las autoridades	SI	Tener contacto frecuente con las autoridades pertinentes
		A.6.1.4	Contacto con grupos de intereses especiales		Tener contacto con áreas y profesionales de seguridad de la información con el fin de mantenerse actualizado
		A.6.1.5	Seguridad de la información en la gestión de proyectos	SI	La seguridad de la información se debe tratar en la gestión de proyectos
	A.6.2: Dispositivos móviles y teletrabajo	A.6.2.1	Política para dispositivos móviles	SI	Se deben adoptar políticas que tengan en cuenta el riesgo que pueden generar el uso de dispositivos móviles dentro de la empresa
		A.6.2.2	Teletrabajo	SI	Se deben adoptar políticas de seguridad para proteger la información a la que tienen acceso los lugares en que se maneja teletrabajo
A.7 Seguridad de los recursos humanos	A.7.1: Antes de asumir el empleo	A.7.1.1	Selección	SI	Se debe tener en cuenta la verificación de antecedentes de los candidatos y solicitar la información reglamentadas por la ley
		A.7.1.2	Términos y condiciones del empleo	SI	Se deben generar acuerdos con los empleados que establezcan responsabilidades en cuando a la seguridad de la información
	A.7.2: Durante la ejecución del empleo	A.7.2.1	Responsabilidades de la dirección	SI	La dirección debe exigir a todos los empleados y contratistas seguir las políticas de seguridad ya establecidas por la organización
		A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	SI	Cada uno de los empleados deben ser informados y educados sobre las políticas de seguridad de la información establecidas por la organización
		A.7.2.3	Proceso disciplinario	SI	Se debe tener proceso definido en caso de que un empleado incumpla las políticas de la seguridad de la información.

	A.7.3: Terminación y cambio de empleo	A.7.3.1	Terminación o cambio de responsabilidades de empleo	SI	Se deben definir las responsabilidades y deberes de los empleados después de terminación o cambio de empleo
A.8 Gestion de activos	A.8.1: Responsabilidad por los activos	A.8.1.1	Inventario de activos	SI	Se deben identificar los activos de información e instalaciones de procesamiento de la información y ,mantener un inventario de estos
		A.8.1.2	Propiedad de los activos	SI	Los activos deben tener un propietario
		A.8.1.3	Uso aceptable de los activos	SI	Se deben crear reglas del buen uso de los activos asociados con información o instalaciones de procesamiento de la información
		A.8.1.4	Devolución de activos	SI	En la terminación de contrato los empleados deben hacer entrega de todos los activos de la organización que tenían a su cargo
	A.8.2: Clasificación de la información	A.8.2.1	Clasificación de la información	SI	Toda la información se debe clasificar según su valor, requisitos legales y susceptibilidad
		A.8.2.2	Etiquetado de información	SI	Se debe desarrollar e implementar procedimientos para el etiquetado de la información
		A.8.2.3	Manejo de activos	SI	Se deben desarrollar e implementar procedimientos para el manejo de activos de acuerdo a la clasificación dada a los mismos
	A.8.3: Manejo de medios	A.8.3.1	Gestión de medios removibles	SI	Se deben implementar procedimientos para la gestión de medios removibles
		A.8.3.2	Disposición de los medios	SI	Se debe disponer de los medios en forma segura cuando ya no se requieran
		A.8.3.3	Transferencia de medios físicos	SI	Los medios que contienen información deben de ser protegidos de accesos no autorizados durante el transporte.
A.9: Control de acceso	A.9.1 Requisitos del negocio para control de acceso	A.9.1.1	Política de control de acceso	SI	Se deben establecer y documentar políticas
		A.9.1.2	Acceso a redes y a servicios en red	SI	Únicamente pueden acceder a la red usuarios autorizados y con los servicios autorizados

	A.9.2 Gestión de acceso de usuario	A.9.2.1	Registro y cancelación del registro de usuarios	SI	Se debe implementar un registro y cancelación formal de usuarios
		A.9.2.2	Suministro de acceso de usuarios	SI	Se debe implementar un suministro de acceso a usuarios y asignar derechos de acceso
		A.9.2.3	Gestión de derechos de acceso privilegiado	SI	Se debe tener un control con la asignación y derechos de usuarios
		A.9.2.4	Gestión de información de autenticación secreta de usuario	SI	La asignación de información de autenticación secreta se debe gestionar de manera formal
		A.9.2.5	Revisión de los derechos de acceso de usuario	NO	Se debe revisar de manera permanente los derecho de acceso de los usuarios
		A.9.2.6	Retiro o ajuste de los derechos de acceso	SI	Los derechos de acceso se deben retirar en el momento que el empleado se retira o se deben ajustar cuando se hagan cambios
	A.9.3 Responsabilidades de los usuarios	A.9.3.1	Uso de información de autenticación secreta	SI	Se debe exigir a los usuarios que cumplan con los requisitos de autenticación secreta
	A.9.4 Control de acceso a sistemas y aplicaciones	A.9.4.1	Restricción de acceso a la información	SI	El acceso a la información y las funciones de los sistemas deben de tener una restricción de acuerdo a las políticas de control de acceso
		A.9.4.2	Procedimiento de ingreso seguro	SI	Cuando es requerido, el acceso al sistema y aplicaciones se debe controlar mediante un acceso seguro
		A.9.4.3	Sistema de gestión de contraseñas	SI	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.
		A.9.4.4	Uso de programas utilitarios privilegiados	SI	Se deben restringir y controlar estrictamente el uso de programas utilitarios que podría anular el sistema y los controles de las aplicaciones.
		A.9.4.5	Control de acceso a códigos fuente de programas	SI	Se debe restringir el acceso al código fuente de los programas
A.10 Criptografí	A.10.1 Controles criptográfico	A.10.1.1	Política sobre el uso de controles criptográficos	SI	Se debe desarrollar e implementar una política sobre el uso de controles

a	s				criptográficos para la protección de la información
		A.10.1.2	Gestión de llaves	SI	Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas
A.11 Seguridad fisica y del entorno	A.11.1 Áreas seguras	A.11.1.1	Perímetro de seguridad física	SI	Se deben definir perímetros de seguridad con el fin de proteger áreas que contengan información confidencial o critica
		A.11.1.2	Controles de acceso físico	SI	Las áreas seguras se deben proteger con el fin que solo puedan acceder a ellas personal autorizado
		A.11.1.3	Seguridad de oficinas, recintos e instalaciones	SI	Se debe diseñar seguridad física a todos los lugares de la organización
		A.11.1.4	Protección contra amenazas externas y ambientales	SI	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes
		A.11.1.5	Trabajo en áreas seguras	SI	Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras
		A.11.1.6	Áreas de despacho y carga	SI	Se deben controlar los espacios de acceso a personal no autorizado y aislar los espacios donde se encuentre información
	A.11.2 Equipos	A.11.2.1	Ubicación y protección de los equipos	SI	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligro del entorno, y las posibilidades de acceso no autorizado.
		A.11.2.2	Servicio de suministro	SI	Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas de suministro
		A.11.2.3	Seguridad del cableado	SI	El cableado se debe proteger contra interceptación, interferencia o daño
		A.11.2.4	Mantenimiento de equipos	SI	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas
		A.11.2.5	Retiro de activos	SI	Los equipos, información o software no se deben retirar sin autorización previa

		A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	SI	Se debe aplicar medidas de seguridad de equipos que se encuentran fuera de las instalaciones
		A.11.2.7	Disposición segura o reutilización de equipos	SI	Se debe asegurar que los equipos no contengan información confidencial, antes de su disposición o reusó
		A.11.2.8	Equipos de usuario desatendido	SI	Se debe asegurar que los equipos desatendidos se les da protección adecuada
		A.11.2.9	Política de escritorio limpio y pantalla limpia	SI	Se deben adoptar políticas de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones.
A.12 Seguridad de las operaciones	A.12.1 Procedimientos operacionales y responsabilidades	a.12.1.1	Procedimientos de operación documentados	SI	Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan
		A.12.1.2	Gestión de cambios	SI	Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
		A.12.1.3	Gestión de capacidad	SI	Se debe hacer seguimiento al uso de recursos, hacer los ajustes y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema
		A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	SI	Se deben separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizado al ambiente de operación
	A.12.2 Protección contra códigos maliciosos	A.12.2.1	Controles contra códigos maliciosos	SI	Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.
	A.12.3 Copias de respaldo	A.12.3.1	Respaldo de la información	SI	Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas y ponerlas a prueba regularmente de acuerdo con

					una política de copias de respaldo acordadas
	A.12.4 Registro y seguimiento	A.12.4.1	Registro de eventos	SI	Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información
		A.12.4.2	Protección de la información de registro	SI	Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado
		A.12.4.3	Registro del administrador y operador	SI	Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad
		A.12.4.4	Sincronización de relojes	SI	Los relojes de todos los sistemas de procesamiento de la información la organización deben de estar en la misma línea de tiempo
	A.12.5 Control de software operacional	A.12.5.1	Instalación de software en sistemas operativos	SI	Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos
	A.12.6 Gestion de vulnerabilidad tecnica	A.12.6.1	Gestión de las vulnerabilidades técnicas	SI	Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen, evaluar la exposición de la organización a estas vulnerabilidades y tomas medidas apropiadas para tratar el riesgo
		A.12.6.2	Restricciones sobre la instalación de software	SI	Se deben establecer e implementar las reglas para la instalación de software por parte de los usuarios
	A.12.7 Consideraciones sobre auditorias de sistemas de información	A.12.7.1	Controles de auditorías de sistemas de información	SI	Los requisitos y actividades de auditoria que involucran la verificación de los sistemas operativos se debe planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio
A.13 Seguridad de las	A.13.1 Gestión de la seguridad de las redes	A.13.1.1	Controles de redes	SI	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones

comunicaciones		A.13.1.2	Seguridad de los servicios de red	SI	Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red
		A.13.1.3	Separación de redes	SI	Los grupos de servicios de información, usuarios y sistemas de información se den separar en las redes
	A.13.2 Transferencia de información	A.13.2.1	Políticas y procedimientos de transferencia de información	SI	Se debe contar con políticas, procedimientos y controles de trasferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.
		A.13.2.2	Acuerdos sobre transferencia de información	SI	Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas
		A.13.2.3	Mensajería electrónica	SI	Se debe proteger adecuadamente la información incluida en la mensajería electrónica
		A.13.2.4	Acuerdos de confidencialidad o de no divulgación	SI	Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información
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	SI	Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información para mejoras a los sistemas
		A.14.1.2	Seguridad de servicios de las aplicaciones en redes publicas	SI	La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se deben proteger de actividades fraudulentas, disputas contractuales, divulgación y modificación no autorizadas
		A.14.1.3	Protección de transacciones de los servicios de las aplicaciones	SI	La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la

					alteración no autorizada de mensajes, la divulgación no autorizada y la duplicación o reproducción de mensajes no autorizada.
	A.14.2 Seguridad en los procesos de desarrollo y de soporte	A.14.2.1	Política de desarrollo seguro	SI	Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización
		A.14.2.2	Procedimientos de control de cambios en sistemas	SI	Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios
		A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	SI	Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, someterlas a prueba
		A.14.2.4	Restricciones en los cambios a los paquetes de software	SI	Se deben desalentar las modificaciones a los paquetes de software los cuales se deben limitar a los cambios necesarios
		A.14.2.5	Principios de construcción de los sistemas seguros	SI	Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros y aplicarlos a cualquier actividad de implementación de sistemas de información.
		A.14.2.6	Ambiente de desarrollo seguro	SI	Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo
		A.14.2.7	Desarrollo contratado externamente	SI	La organización debe supervisar y hacer seguimiento del desarrollo de sistemas contratado externamente
		A.14.2.8	Pruebas de seguridad de sistemas	SI	Durante la prueba se deben llevar a cabo pruebas de funcionalidad de la seguridad
		A.14.2.9	Pruebas de aceptación de sistemas	SI	Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para la

					aceptación y criterios de aceptación
	A.14.3 Datos de prueba	A.14.3.1	Protección de datos de prueba	SI	Los datos de prueba se deben seleccionar proteger y controlar cuidadosamente
A.15 Relaciones con los proveedores	A.15.1 Seguridad de la información en las relaciones con los proveedores	A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	SI	Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se den acordar con estos y se deben documentar
		A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	SI	Se deben establecer todos los requisitos de seguridad de la información para cada proveedor que pueda tener acceso.
		A.15.1.3	Cadena de suministro de tecnología de información y comunicación	SI	Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministros de productos y servicios de tecnología de información y comunicación
	A.15.2 Gestión de la prestación de servicios de proveedores	A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	SI	La organización debe hacer seguimiento revisar y auditar con regularidad la prestación de servicio de los proveedores
		A.15.2.2	Gestión de cambios en los servicios de los proveedores	SI	Se deben gestionar 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
A.16 Gestion de incidentes de seguridad de la informacion	A.16.1 Gestion de incidentes y mejoras en la seguridad de la informacion	A.16.1.1	Responsabilidades y procedimientos	SI	Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de a información.
		A.16.1.2	Reporte de eventos de seguridad de la información	SI	Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados
		A.16.1.3	Reporte de debilidades de seguridad de la información	SI	Se debe exigir a todos los miembros de la organización y proveedores que utilizan los sistemas de información, dar conocimiento de cualquier

					debilidad de seguridad de la información observada o sospechada.
		A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones entre ellos	SI	Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad
		A.16.1.5	Respuesta a incidentes de seguridad de la información	SI	Sedar respuesta a los incidentes de seguridad de la información de acuerdo a los procedimientos documentados
		A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	SI	El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se deben usar para disminuir la posibilidad o impacto de incidentes futuros
		A.16.1.7	Recolección de evidencias	SI	La organización debe definir y aplicar para la identificación recolección, adquisición y preservación de información que pueda servir como evidencia
A.17 Aspectos de seguridad de la información de la gestion de continuidad de negocio	A.17.1 Continuidad de la información	A.17.1.1	Planificación de la continuidad de la seguridad de la información	SI	La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas
		A.17.1.2	Implementación de la continuidad de la seguridad de la información	SI	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa
		A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	SI	La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situación adversas
	A.17.2 Redundancias	A.17.2.1	Disponibilidad de instalaciones de procesamiento	SI	Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para

			de información		cumplir los requisitos de disponibilidad
A.18 Cumplimiento	A.18.1 Cumplimiento de requisitos legales y contractuales	A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	SI	Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización
		A.18.1.2	Derechos de propiedad intelectual	SI	Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos , de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados
		A.18.1.3	Protección de registros	SI	Los registros se deben proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos y la reglamentación pertinente.
		A.18.1.4	Privacidad y protección de información de datos personales	SI	Se debe asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinente
		A.18.1.5	Reglamentación de controles criptográficos	SI	Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinente
	A.18.2 Revisiones de seguridad de la información	A.18.2.1	Revisión independiente de la seguridad de la información	SI	El enfoque de la organización para la gestión de seguridad de la información y su implementación, se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos
		A.18.2.2	Cumplimiento con las políticas y normas de seguridad	SI	Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de

					información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas y cualquier otro requisito de seguridad
		A.18.2.3	Revisión del cumplimiento técnico	SI	Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información

Tabla 6 Tratamiento de riesgos y controles

14. ANALISIS DE BRECHA GAP

El análisis de brechas es una herramienta de análisis para comparar el estado y desempeño real de una organización, estado o situación en un momento dado, respecto a uno o más puntos de referencia seleccionados de orden local, regional, nacional y/o internacional.

El resultado esperado es la generación de estrategias y acciones para llegar al referente u objetivo futuro deseado.

Para llevar a cabo el análisis de brechas se realizan cuatro pasos generales y cómo guía cada paso busca responder una pregunta:

1. Decidir cuál es la situación actual que se desea analizar ("lo que es") y que se quiere resolver. En este paso se responde a la pregunta: ¿Dónde estamos?
    - Actualmente SALUDVIDA EPS, se encuentra en proceso de realización de un sistema de gestión de seguridad de la información, se tienen las herramientas necesarias para realizar los controles exigidos por la norma y se está en proceso de documentación, por lo que el presente proyecto será una base para la realización de la misma, en el momento de ingreso a la compañía con un estado de avance del 70% aproximadamente.

2. Delinear el objetivo o estado futuro deseado ("lo que debería ser"). Respondería la pregunta ¿Con la practica a donde deberíamos llegar?
    - Con el presente proyecto se busca avanzar en la realización del sistema de gestión de seguridad de la información, sirviendo como insumo principalmente en la parte documental y análisis de riesgos y vulnerabilidades, pues gran parte de los controles exigidos ya se encuentran en ejecución y perfeccionamiento.
3. Identificar la brecha entre el estado actual y el objetivo. Responde a la pregunta ¿Cuán lejos estamos de donde queremos estar?
    - Teniendo en cuenta que la empresa se encuentra en perfeccionamiento de los controles y analizando posibles riesgos y amenazas, espero con el presente proyecto tener un avance del 10%, teniendo así un porcentaje final del 90%.
4. Determinar los planes y las acciones requeridas para alcanzar el estado deseado Responde a la pregunta de ¿Cómo llegamos fin planteado?:
    - Se realiza principalmente un análisis en la que se busca mejorar lo que está establecido en la empresa y con el presente proyecto servir como insumo documental para cumplir con lo exigido en la norma, siendo un apoyo significativo para el área de seguridad de la información de SALUDVIDA EPS.

En el ejercicio de las prácticas se puede observar el nivel de madurez en que se encuentra actualmente SALUDVIDA EPS respecto a la seguridad de la información donde el objetivo primordial es el diseño de un sistema de gestión de seguridad de la información, que facilite la meta próxima del área que es la certificación en la norma ISO/IEC 27001; para dicho propósito

se diseña en primer lugar un análisis de brecha GAP, en el cual se evalúa el estado inicial y al cual se quiere llegar con la pasantía, evaluando los requisitos de un sistema de gestión de seguridad de la información, frente al actual estado de la compañía para lograrlo.

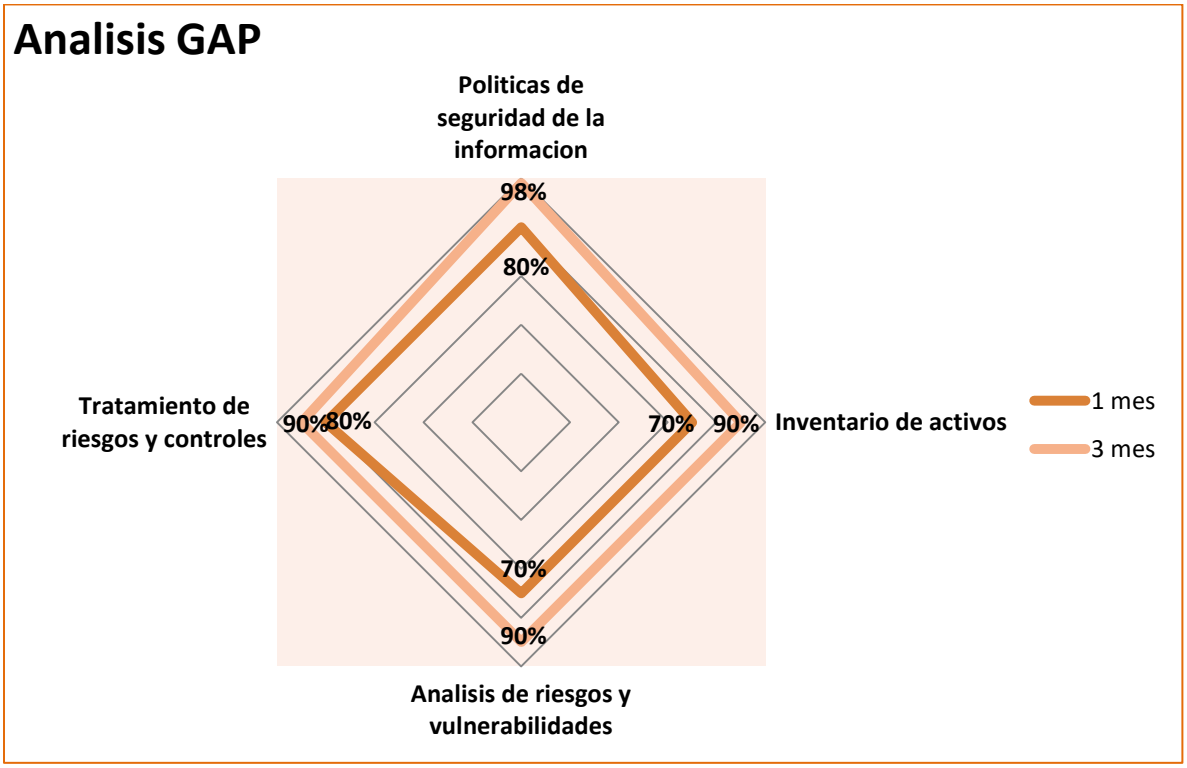


Tabla 7 Análisis GAP

CONTROLES DE SEGURIDAD DE LA INFORMACION	1 mes	3 mes
Definición de alcance	50%	80%
Políticas de seguridad de la información	80%	98%
Inventario de activos	70%	90%
Análisis de riesgos y vulnerabilidades	70%	90%
Tratamiento de riesgos y controles	80%	90%

Tabla 8 Avance

Con este análisis se encuentra que los requisitos básicos para la implementación del SGSI, se encontraba en un 70% teniendo claro cada uno de los puntos para la planeación pero no debidamente documentados por lo que con el presente informe se llega al 90%, de avance siento un apoyo significativo.

RESULTADOS:

Después del periodo de 13,3 semanas se concluye el tiempo de pasantía logrando el objetivo principal obteniendo un diseño de gestión de seguridad de la información (SGSI) apalancado en la norma ISO/IEC 27001 en su fase de planeación y un mejoramiento general de la seguridad de la información en SALUDVIDA EPS del 10%.

15. CONCLUSIONES

Aunque SALUDVIDA EPS, cuenta con una buena gestión de seguridad de la información, es un trabajo que tal como lo dice la norma ISO/IEC 27001 requiere de un continuo mejoramiento y evolución ya que cada día aparecen nuevas y mejores formas de atacar la información de las empresas, en la realización de las practicas se logra concientizar de la importancia de la seguridad de la información y como una buena gestión de misma, puede garantizar una reducción significativa de potenciales riesgos.

Se puede establecer que en general los funcionarios desconocen la importancia de la seguridad de la información y no comprenden el porqué de muchos controles, se debe reforzar en la capacitación y concientización.

16. BIBLIOGRAFÍA

Alegsa, L. (05 de 12 de 2010). *Definición de Ataque informático*. Obtenido de Alegsa.com.ar: http://www.alegsa.com.ar/Dic/ataque_informatico.php

Ballén, X. R. (Agosto de 2012). *ANALISIS_BRECHAS_administrativos guia290812.* Obtenido de Universidad Nacional de Colombia: http://www.odontologia.unal.edu.co/docs/claustros-colegiaturas_2013-2015/Guia_Analisis_Brechas.pdf

colombiacompra.gov.co. (23 de Junio de 2016). *Alcance del Sistema de Gestión de Seguridad de la Información.* Obtenido de https://www.colombiacompra.gov.co/sites/cce_public/files/cce_documentos/20160623alcancedelsgsi.pdf

EDP. (Marzo de 2017). *Política de Seguridad de la Información aplicable a proveedores de.* Obtenido de https://www.edphcenergia.es/recursosedp/doc/portal-institucional/20130820/proveedores/politica-de-seguridad-de-la-informacion-para-proveedores-de-edp-en-espana.pdf

ESE SALUD PEREIRA. (Mayo de 2017). *Registro de activos de información.* Obtenido de http://www.saludpereira.gov.co/medios/ESE_-_Activos_de_Informacion_v02_1.pdf

Excellence, I. (15 de 03 de 2015). *ISO 27001: Los activos de información*. Obtenido de SGSI Blog especializado en Sistemas de Gestión : https://www.pmg-ssi.com/2015/03/iso-27001-los-activos-de-informacion/

FINAGRO Fondo para el financiamineto del sector agropecuario. (08 de 2018). *Inventario de activos de información.* Obtenido de https://www.finagro.com.co/qui%C3%A9nes-somos/activos-de-informaci%C3%B3n

ICETEX. (Octubre de 2014). *MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN.* Obtenido de https://www.icetex.gov.co/dnnpro5/Portals/0/Documentos/La%20Institucion/manuales/Manualseguridadinformacion.pdf

ICONTEC. (2006). *NORMA TECNICA NTC-ISO/IEC COLOMBIANA 27001.* Bogota.

Incibe. (s.f.). *Proteje tu empresa.* Obtenido de ¿Que te interesa? Plantilla ejemplo para inventario de activos: https://www.incibe.es/protege-tuempresa/que-te-interesa/plan-director-seguridad

intelectual, O. O. (s.f.). *Derecho de autor*. Obtenido de http://www.wipo.int/copyright/es/

Luján, U. N. (s.f.). *Glosario*. Obtenido de Departamento de Seguridad Informática: http://www.seguridadinformatica.unlu.edu.ar/?q=lexicon/1

PLANEACION, O. D. (Octubre de 2017). *Políticas de Seguridad de la información.* Obtenido de AUDITORÍA GENERAL DE LA REPUBLICA DE COLOMBIA: http://www.auditoria.gov.co/Biblioteca_documental/Politicas/TI.120.P01.A07_Anexo%207%20Politicas%20de%20Seguridad.pdf

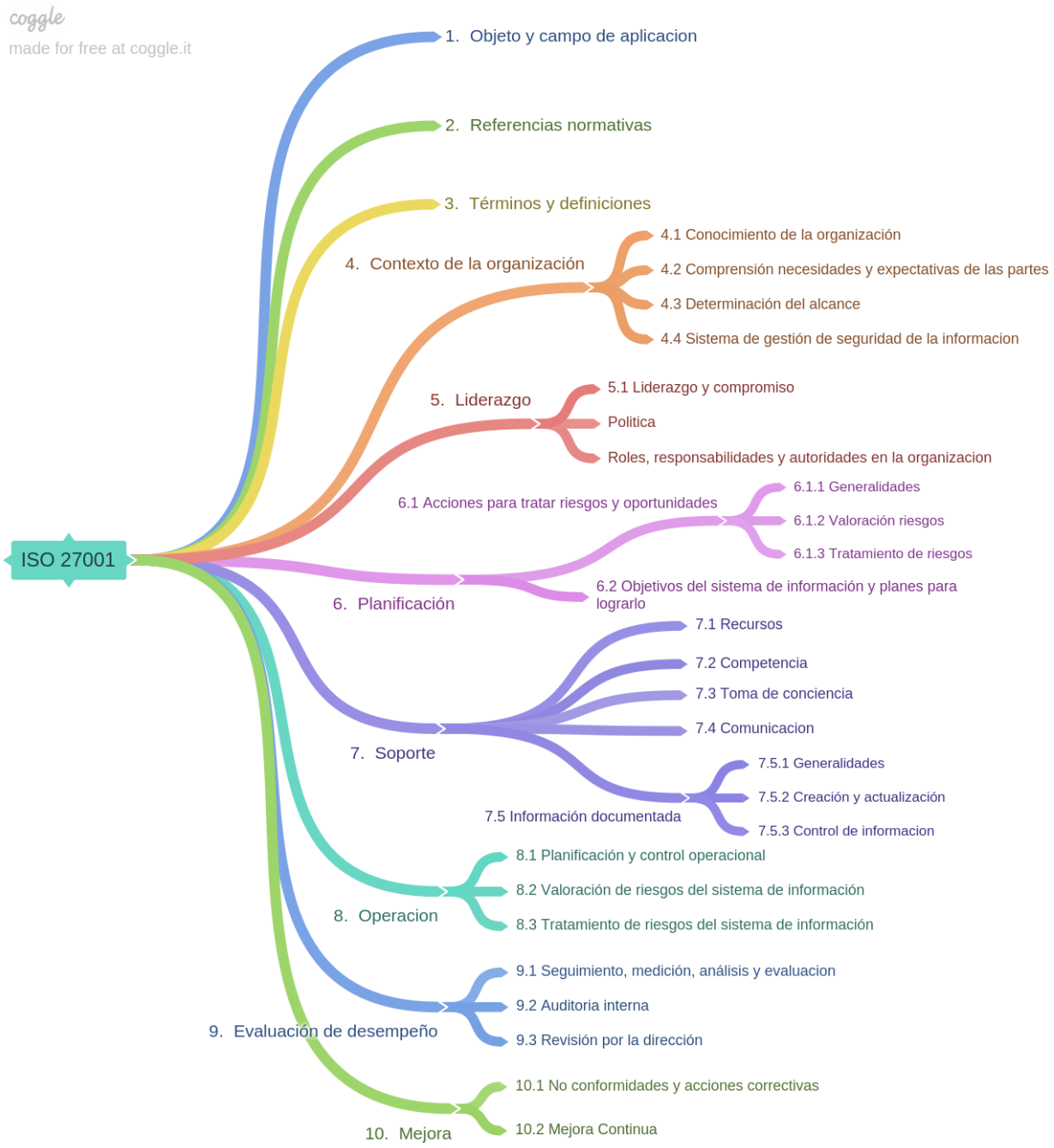
REPUBLICA, A. G. (10 de 2017). *Políticas de Seguridad de la información.* Obtenido de http://www.auditoria.gov.co/Biblioteca_documental/Politicas/TI.120.P01.A07_Anexo%207%20Politicas%20de%20Seguridad.pdf

SALUDVIDA. (Agosto de 2018). *La entidad*. Obtenido de https://www.saludvidaeps.com/index.php/corporativo/la-entidad

TECON. (01 de 2018). *POLÍTICA GLOBAL DE SEGURIDAD DE LA INFORMACIÓN* . Obtenido de https://tecon.es/wp-content/uploads/2018/03/POLITICA-ISO-27001-2014.pdf

WIKIPEDIA. (18 de 02 de 2018). *Sistema de gestión de la seguridad de la información*. Obtenido de https://es.wikipedia.org/wiki/Sistema_de_gesti%C3%B3n_de_la_seguridad_de_la_informaci%C3%B3n

ANEXO 1


coggle
made for free at coggle.it
ISO 27001
1. Objeto y campo de aplicacion
2. Referencias normativas
3. Términos y definiciones
4. Contexto de la organización
4.1 Conocimiento de la organización
4.2 Comprensión necesidades y expectativas de las partes
4.3 Determinación del alcance
4.4 Sistema de gestión de seguridad de la informacion
5. Liderazgo
5.1 Liderazgo y compromiso
Politica
Roles, responsabilidades y autoridades en la organizacion
6. Planificación
6.1 Acciones para tratar riesgos y oportunidades
6.1.1 Generalidades
6.1.2 Valoración riesgos
6.1.3 Tratamiento de riesgos
6.2 Objetivos del sistema de información y planes para lograrlo
7. Soporte
7.1 Recursos
7.2 Competencia
7.3 Toma de conciencia
7.4 Comunicacion
7.5 Información documentada
7.5.1 Generalidades
7.5.2 Creación y actualización
7.5.3 Control de informacion
8. Operacion
8.1 Planificación y control operacional
8.2 Valoración de riesgos del sistema de información
8.3 Tratamiento de riesgos del sistema de información
9. Evaluación de desempeño
9.1 Seguimiento, medición, análisis y evaluacion
9.2 Auditoria interna
9.3 Revisión por la dirección
10. Mejora
10.1 No conformidades y acciones correctivas
10.2 Mejora Continua