PLAN DIRECTOR DE SEGURIDAD DE LA INFORMACIÓN UESMA

Francisco Xavier Quiñonez Angulo

Maestría en Seguridad de las Tecnologías de la Información

Sistemas de Gestión de Seguridad de la Información

Profesor Colaborador: Antonio Jose Segovia Henares

TRABAJO REALIAZADO EN LA UNIDAD EDUCATIVA SALESIANA MARIA PREVIO A LA OBTENCIÓN DEL TITULO DE MAGISTER EN SEGURIDAD DE LAS TICS

2019 - 2020

RESUMEN

El presente proyecto consiste en la elaboración de un Sistema Gestor de Seguridad de la información en el cual se establecen varias metodologías para su elaboración, enmarcado todo en el conocido ciclo de Deming para poder garantizar el cumplimiento y actualización del SGSI.

La UESMA es una institución educativa de Esmeraldas Ecuador que forma parte de una cadena de centros escolares repartidas en todo el mundo, es aquí donde se lleva a cabo la ejecución del SGSI.

A través de la fase de 1 en la cual se contempla el análisis referencial se pudo constatar que la situación de la Unidad Educativa Salesiana María Auxiliadora frente a la seguridad de la información desglosada en los requisitos que establece la ISO 27001 y los controles del Anexo A determinar que la situación es crítica y es necesario la implementación del Sistema Gestor de Seguridad de la Información con el fin de hacer prevalecer la seguridad de la información y salvaguardar los activos y sistemas informáticos frente a cualquier eventualidad de ocurrencia de un desastre por menor que parezca, es por ello que en esta misma fase se establece el alcance del SGSI en la cual quedan señalados todos los activos informáticos de la institución y los procesos asociados a los mismos.

En la fase denominada sistema de gestión documental se establecen las políticas de seguridad de la información basadas en la legislación ecuatoriana relacionada con la seguridad de la información y el tratamiento de los datos, es en esta fase donde queda estructurada el contorno de la protección de datos, derechos y deberes de los empleados y clientes, enmarcados en el campo de educación continua. Luego de establecer la metodología para el análisis de riesgos se enfatiza en los responsables de esta labor y el comité de seguridad establece los indicadores para determinar cuándo un activo de información, contemplado en el alcance se considera de riesgo y la respectiva aprobación de los directivos para proceder a ejecutar el exhaustivo inventario de activos de análisis de riesgos.

Establecido todo el contexto necesario se procede a realizar el inventario de activos en el cual se identifican un total de 1610 activos distribuidos en 46 apartados dentro de 8 tipos de activos en la UESMA, mismos que necesitan ser analizado el riesgo y las etapas posteriores como tratamiento del riesgo y modificación del mismo de ser necesario, basados en el riesgo aceptable para la institución establecido por el comité de seguridad y aprobado por los directivos mismo que determina el impacto potencial y el riesgo

residual incorporados a cada una de las amenazas detectadas y las vulnerabilidades encontradas en la institución.

Conociendo los activos que superan el riesgo aceptable y los que están próximos a alcanzar este umbral de riesgo se plantean diversos proyectos que en su mayoría necesita de inversión económica para que permitan llevar el impacto potencial sobre los activos mencionados a un nivel aceptable y se evidencia que estos proyectos no solo generan una afectación positiva sobre los activos que se consideran para realizar el tratamiento de riesgos sino también en los demás y el resultado obtenido sobre estos proyectos supera las expectativas establecidas puesto que para algunos activos se logró erradicar el riesgo y a otras se los llevó a un nivel muy por debajo del aceptable.

Finalmente, la fase 5 de este TFM y SGSI es la de auditoria, en la cual mediante la metodología de Modelo de Madurez de Capacidades (CMM) y la ISO 27002 que permite analizar el cumplimiento de las necesidades que establece la ISO 27001 para garantizar la seguridad de la información, presentan que la Unidad Educativa Salesiana María Auxiliadora ha logrado una importante evolución en el marco de la seguridad de la información, es decir la ejecución de los proyectos y controles detallados en las fases anteriores brindan el resultado esperado, no obstante se realizan algunas recomendaciones para optimizar el SGSI y demostrar mayor madurez al respecto.

Índice

Índice de tablas

Índice de ilustraciones

0. GLOSARIO

PTR: Plan de Tratamiento de Riesgos, es aplicar controles sobre los riesgos identificados.

SI: Seguridad de la Información

SGSI: Sistema Gestor de Seguridad de la Información, conjunto de políticas de administración de la seguridad de sistemas informáticos.

TIC: Tecnologías de la Información y la Comunicación.

PCN: Plan de Continuidad de Negocio, es el conjunto de normas de cómo se debe recuperar y restaurar las funciones en una empresa.

CISO: Chief Information Security Officer, oficial de la seguridad de la información.

UESMA: Unidad Educativa Salesiana María Auxiliadora

Contingencia: Suceso que puede suceder o no, especialmente un problema que se produce de manera imprevista.

Integridad: Correctitud y completitud de la información.

Disponibilidad: La información o sistemas son accesibles cuando son necesarios.

Confidencialidad: Característica de la información que es únicamente accesible por el personal autorizado.

Riesgos: Posibilidad de que se produzca un incidente, o posibilidad de que una amenaza explote una vulnerabilidad.

Amenazas: Persona, configuración, proceso, objeto o acontecimiento que puede causar perjuicio.

Vulnerabilidad: Debilidad o falla en un sistema de información que da la posibilidad a que una amenaza se materialice.

Consecuencia: Acontecimiento resultante de la materialización de un riesgo.

Control: Proceso por el cual se intentar tener una información precisa para tomar decisiones o evitar que algo suceda.

Indicadores: Característica observable y medible que puede ser usada para mostrar progresos y cambios que se pueden estar efectuando en algo.

Periodicidad: Frecuencia en el tiempo con la que aparece, sucede o se realiza algo.

Probabilidad: Posibilidad de que se realice algo.

Mitigación: Reducir al mínimo la probabilidad de que ocurra una vulnerabilidad o que no afecte en el funcionamiento de algo.

Auditoría: Proceso realizado por profesionales para constatar el cumplimiento o no de algo.

Gestión: Asumir y llevar a cabo las responsabilidades sobre un proceso.

Estrategia: Serie de acciones meditadas que buscan la consecución de un fin determinado.

Activo: Bien o servicio con capacidades funcionales y operativas.

Avería: Daño, rotura o fallo que impide o perjudica el funcionamiento de un dispositivo.

Impacto: Efecto que se produce tras materializarse o producirse un riesgo.

VLAN: Red de área local virtual.

LAN: Red de área local.

Router: Dispositivo físico que permite interconectar y enrrutar en red varias computadoras o redes de computadoras.

Switch: Conmutador usado en la interconexión de computadoras.

Servidor: Software que realiza ciertas tareas, o equipo con propósito de proveer datos o aplicaciones para que sea usada por otras máquinas.

GTH: Departamento/persona responsable de la gestión de talento humano en la institución.

DPEI: Departamento/persona responsable de la planeación y evaluación institucional.

AAA: Autenticación, autorización y contabilización.

CMM: Modelo de Madurez de Capacidades.

0.1 DESCRIPCIÓN

El Plan Director de Seguridad de la Información es un conjunto de procesos y actividades de gran importancia para una organización sin importar el sector productivo al que pertenezca, simplemente los directivos buscan alinear sus objetivos institucionales de la mano de los servicios de información, en estos casos se debe garantizar la seguridad de estos activos para evitar pérdidas de información o crear una mala imagen de la empresa referente a los procesos relacionados con las TICS.

Este proyecto pretende establecer las bases y lineamientos necesarios, fundados en estándares internacionales, para salvaguardar la seguridad de los servicios de información y la continuidad de negocio en la Unidad Educativa Salesiana María Auxiliadora. Este documento abordará las siguientes etapas para su consecución:

- Documentación normativa sobre las mejores prácticas en seguridad de la información.
- Definición clara de la situación actual y de los objetivos del SGSI.
- Análisis de Riesgos.
    - Identificación y valoración de los activos.
    - Identificación de amenazas, evaluación y clasificación de las mismas
- Evaluación del nivel de cumplimiento de la ISO/IEC 27002:2013 en la organización.
- Propuestas de proyectos de cara a conseguir una adecuada gestión de la seguridad.
- Esquema Documental.

Los entregables de este proyecto se fracciona en seis fases, mismas que serán entregadas en el siguiente orden cronológico, es decir no se puede avanzar a una fase si no se ha cumplido la anterior:

- Informe Análisis Diferencial
- Esquema Documental ISO/IEC 27001
- Análisis de Riesgos
- Plan de Proyectos
- Auditoría de Cumplimiento
- Presentación de resultados

0.2 METODOLOGÍA

Para la elaboración de este plan director de seguridad, en varias etapas del mismo se recurre a estándares, metodologías, técnicas y procedimientos reconocidos internacionalmente y utilizados por la industria, entre los cuales se detallan los siguientes:

ISO/IEC 27000: Es un vocabulario estándar para los Sistemas de Gestión de Seguridad de la Información, brinda una introducción esencial para el resto de la serie. Actualmente se encuentra en la quinta versión actualizada en febrero del 2018.

Contiene un conjunto de buenas prácticas para el establecimiento, implementación, mantenimiento y mejora de Sistemas de Gestión de la Seguridad de la Información enfatiza la importancia del mismo sin importar el tamaño y/o tipo de empresa. A continuidad en la serie se presentan:

ISO/IEC 27001: Define los requisitos indispensables para establecer, implantar, mantener y mejorar un SGSI.

ISO/IEC 27002: Proporciona recomendaciones de las mejoras prácticas en la gestión de la seguridad de la información, basándose en los tres ejes fundamentales: confidencialidad, integridad y disponibilidad.

ISO/IEC 27004: Establece lineamientos para ayudar a organizaciones a evaluar el rendimiento de la seguridad de la información y la eficiencia de un sistema de gestión para que se cumpla

ISO/IEC 27005: Suministrar directrices para la gestión de riesgos de seguridad de la información de una empresa.

ISO/IEC 27007: Es una guía para auditar y evaluar la efectividad SGSI.

ISO/IEC 27016: Esta norma se concentra en el análisis financiero y económico de equipos y procedimientos involucrados en un incidente de seguridad.

ISO/IEC 27031: Guía de continuidad del negocio en procesos relacionados a las TICS.

ISO/IEC 27035: Presenta un enfoque de actividades y procesos orientados al tratamiento de los incidentes en la seguridad de la información.

ISM3: Es un estándar que permite a la organización la continuidad en sus procesos cuando se presenta algún inconveniente de seguridad, estableciendo métricas para

establecer los niveles de seguridad, se basa en el lema publicado por Josue Perez. "Lo que no se puede medir, no se puede gestionar, y lo que no se puede gestionar, no se puede mejorar".

ITIL: Information Technology Infraestructure Library y en español Biblioteca de Infraestructura de Tecnologías de la Información, es un conjunto de buenas prácticas para la gestión de servicios TI, fue creado para orientar en la administración de servicios de TI y basado en la seguridad de la información proyecta minimizar el riego.

COSO (Committee of Sponsoring Organizations of the Treadway) es una agrupación voluntaria conformada por cinco organizaciones privadas de Estados Unidos, tienen como objetivo proporcionar una guía potencial que involucra tres temas interrelacionados: la gestión del riesgo empresarial (ERM), el control interno, y la disuasión del fraude. Actualmente se encuentra la versión COSO III desde mayo del 2013.

MAGERIT: Metodología de Análisis de Riesgos de los Sistemas de Información, elaborada por el Consejo Superior de Administración Electrónica del Gobierno de España y tiene como propósito minimizar los riesgos al implementar y usas tecnologías de la información. Actualmente se encuentra en su versión 3 publicada en el año 2012.

Systems Security Engineering Capability Maturity Model (SSE-CMM): En español Modelo de Madurez de Capacidades en la Ingeniería de Seguridad de Sistemas, es una derivación del CMM, el cual describe las particularidades fundamentales en procesos para salvaguardar la seguridad de la información en una organización. Su versión actual es la v3.0 la cual fue publicada en junio de 2003.

MECI: Sus siglas significan Modelo Estándar de Control Interno. El MECI es una herramienta gerencial que tiene como fin servir de control de controles para que las entidades del Estado logren cumplir con sus objetivos institucionales y con el marco legal aplicable a ellas.

Los estándares previamente mencionados serán empleados en diferentes fases y partes de este Trabajo Final de Master, teniendo en cuenta la descripción de la empresa en la fase de contextualización de este documento y detallada a continuación.

Los modelos ISO proveen una serie minuciosa de procedimientos que se adaptan a cualquier tipo de empresa sin importar los fines ni la magnitud de la misma, el estándar ISM3 permite garantizar la continuidad del negocio en busca de los objetivos de la institución pese a los incidentes presentados en la seguridad de la información y se adapta a la serie ISO 27000.

ITIL permite establecer buenas prácticas para la correcta administración de los sistemas de información, a través de COSO se identificará la situación de riesgo que presenta la institución, correlacionado con el control interno y los fraudes que se pueden presentar en la corrupción de la información en los activos críticos. La metodología SSE-CMM pretende establecer procesos fundamentales y espontáneos para el aseguramiento de la información mientras que MECI debe ser empleado para realizar los controles de seguridad en los equipos y servicios otorgados por el estado, al ser la UESMA una institución mixta (Privada y fiscal).

0.2.1 PLAN DO CHECK ACT (PDCA).

Un destacable número de autores establecen que en conjunto con las normas ISO 27001 y la ISO 27002 se debe utilizar el ciclo de Demming, con el propósito de garantizar la mejora continua.

Ilustración 1:Plan Do Check Act.

P – Plan – Panificar: En esta primera etapa es donde se establecen las actividades a realizar en el SGIS, entre sus tareas destacan:

- ✓ Establecer la política de seguridad
- ✓ Delimitar el alcance.
- ✓ Identificar la institución.
- ✓ Constituir los objetivos del SGSI.
- ✓ Identificar los activos.
- ✓ Definir los riesgos.

D – Do – Hacer: Una vez conocidos los lineamientos, en esta fase se ejecutan las salvaguardas de seguridad, básicamente es ejecutado un plan de gestión de incidentes y asociados a indicadores que permitan conocer la efectividad de los mismos.

C – Check – Verificar: Es necesario evaluar la garantía que presta el plan director de seguridad, este proceso se lo realiza a través de una auditoria interna, misma que proporcionará como resultado que tan factible es el proceso realizado.

A – Act – Actuar: Teniendo en cuenta el resultado de la fase anterior, en esta se establecen procesos de mejoras que permitirán corregir los errores detectados.

1. FASE 1

1.1 INTRODUCCIÓN

El Plan Director de Seguridad es uno de los elementos clave con que debe trabajar el Responsable de Seguridad de una organización. Este plan constituye la hoja de ruta que debe seguir la empresa para gestionar de una forma adecuada la seguridad, permitiendo no sólo conocer el estado de la misma, sino en qué líneas se debe actuar para mejorarla. Estamos hablando por tanto de un modelo de mejora continua PDCA (Plan-Do-Check-Act).

El presente proyecto pretende proponer un Plan Director de Seguridad de la Información en la Unidad Educativa Salesiana María Auxiliadora, el cual pretende establecer un conjunto de actividades y procesos que permitan conocer las necesidades de la institución en materia de seguridad de la información.

Una vez identificadas las necesidades de la UESMA se deben identificar los activos de información en orden de criticidad e importancia para la institución para así encontrar sus vulnerabilidades y amenazas para posteriormente establecer mecanismos que impidan el malfuncionamiento o perdida en los sistemas de información.

Para esto es necesario efectuar un previo análisis, que debe estar basado en un conjunto de estándares internacionales reconocidos por la industria donde se identifiquen y clasifiquen los activos, las principales amenazas que afectan a la institución y el riesgo coligado a cada una de ellos, basados en la posibilidad y el impacto que posean de materializarse.

Para mitigar el riesgo de estas amenazas se pretende establecer varios puntos de acción compendiados en procesos y actividades que formarán parte del plan director, teniendo en cuenta que en la institución no existen políticas ni procesos para

salvaguardar la información asociada a un dispositivo o sistema informático, y es evidente que por la magnitud de la UESMA y la importante dependencia con las TICS es una potencial víctima de ataques informáticos.

Al concluir este TFM la Unidad Educativa Salesiana María Auxiliadora podrá identificar de manera clara y concisa sus activos en orden de relevancia, conocer qué tipo de amenazas y vulnerabilidades los asechan, también se pretende sugerir una serie de procesos, actividades y documentos que permitan mitigar los riesgos existentes.

1.2.1 DESCRIPCIÓN DEL NEGOCIO

Unidad Educativa Salesiana María Auxiliadora (UESMA), es una institución educativa que actualmente dispone de 193 empleados (entre docentes y personal administrativo) y 3247 estudiantes, se encuentra ubicada en el sur de la ciudad de Esmeraldas desde el año 1992, su oferta académica va desde primer año de básica hasta tercer año de bachillerato, sus especialidades son mecanizado y construcciones metálicas, instalaciones de equipos y máquinas eléctricas e informática.

En la entrevista con el director de esta comunidad educativa, Padre Pedro Vidal Rocuant Sdb, se le cuestionó sobre cómo podría describir la institución y detalló: “Nuestro proyecto educativo salesiano exige la convergencia de intenciones y de convicciones por parte de todos sus miembros. Por eso, la necesidad de una auténtica Comunidad Educativo-Pastoral que sea a la vez sujeto y ambiente de educación siempre a la vanguardia de los avances tecnológicos y directamente dependiente de estos en su funcionamiento. En esta, todos nos sentimos corresponsables de la calidad educativa del centro y de la realización personal y social de cada uno de sus miembros.

Se definen como:

- Comunidad: porque implica en un clima de familia a estudiantes, padres, educadores y personal.
- Educativa: porque ayuda a desarrollar las posibilidades de los jóvenes en todos los aspectos: culturales, profesionales y sociales.
- Pastoral: porque acompaña a los jóvenes en su maduración cristiana.

Misión

Somos una institución con carisma salesiano que brinda un proyecto de formación integral orientado a Cristo, hombre perfecto, y la pedagogía de don Bosco para satisfacer las necesidades educativas de la niñez y juventud esmeraldeña para que transformen su realidad y cuiden el ambiente que les rodea.

Visión

La Unidad Educativa Fiscomisional María Auxiliadora de Esmeraldas al año 2022, proveerá a la comunidad una educación basada en un aprendizaje sostenible y en el sistema preventivo de Don Bosco, que utilice las TIC, fomente la identidad cultural, deportiva, investigativa, creativa, ambiental e inclusiva; y garantiza una formación sólida en valores, ciudadanía, identidad personal, regional y nacional; cuidando y preservando el medio ambiente, para formar estudiantes de diversos sectores sociales como buenos cristianos y honrados ciudadanos.

La Comunidad Educativa de la UEFMA, edifica el Ideario Institucional en los cimientos de una Comunidad Educativo-Pastoral Salesiana, partiendo de la identificación de esta y la estructuración de políticas, principios y valores con el compromiso de potenciar el proceso educativo centrado en el ser humano.

Organigrama

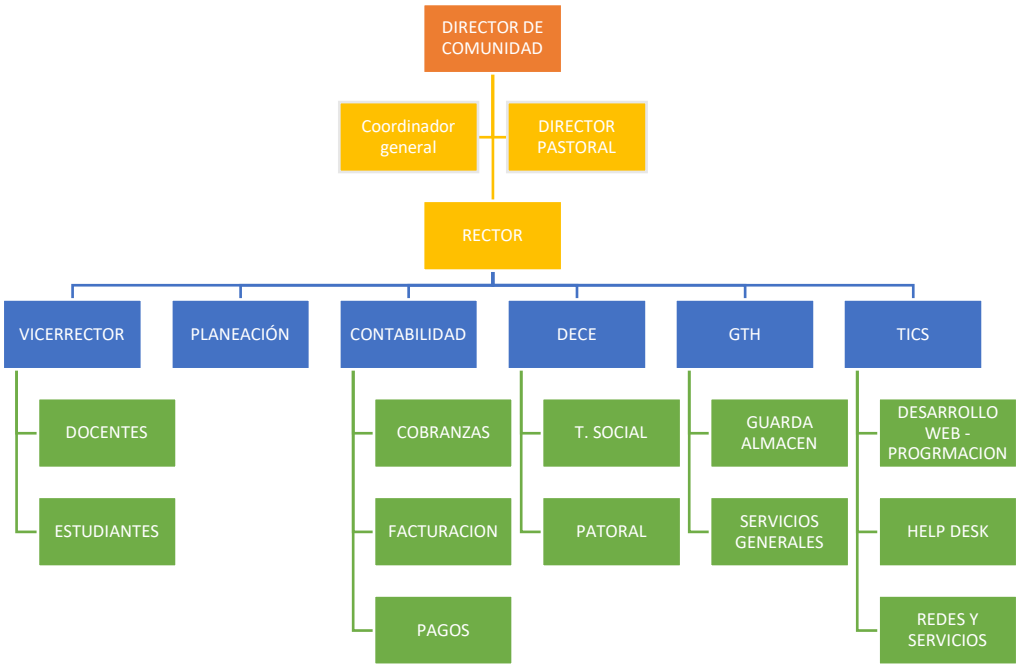

Ilustración 2: Organigrama institucional

Este proyecto está enfocado en proponer mecanismos, procesos y metodologías que permitan a la institución solventar los incidentes de seguridad relacionados a los diferentes sistemas de información usados en varios de los departamentos y procesos de la UESMA. Para poder concluir con las metodologías ya expuestas en el tiempo

estipulado en la planificación, se dará por hecho que las medidas de seguridad propuestas fueron ejecutadas.

1.2.2 OBJETIVOS DEL PLAN DIRECTOR

GENERAL

Elaborar un Plan Director de seguridad de la información para la Unidad Salesiana María Auxiliadora mediante el uso de estándares internacionales de cyber seguridad que permitan garantizar la integridad, confidencialidad de la información y la continuidad de negocio.

ESPECIFICOS

- ✓ Identificar los activos de información y su nivel de importancia en la institución para jerarquizarlos y definir los niveles de seguridad en cada uno.
- ✓ Analizar los riegos y amenazas a través de estándares que permitan conocer la incidencia en cada uno de los activos de información.
- ✓ Realizar análisis que permitan conocer la situación actual y las vulnerabilidades presentes en los activos de información de la UESMA.
- ✓ Establecer estrategias, procesos y equipos informáticos que permitan mitigar los riesgos, amenazas y vulnerabilidades para garantizar la seguridad tecnológica en la institución.

SEGURIDAD DE LA INFORMACIÓN (SI)

- ✓ Salvaguardar los activos de información de la UESMA basándose en los principios de confidencialidad, integridad y disponibilidad.
- ✓ Alinear de manera estratégica la seguridad de la información con la consecución de los objetivos institucionales.
- ✓ Utilizar un enfoque de sistemático para planificar, implementar, monitorizar y gestionar los incidentes de los sistemas de información garantizando la continuidad del negocio.

1.3 ALCANCE DEL SGSI

Ahora ya definidos los objetivos del Plan Director de Seguridad de la Información, es importante precisar los límites del presente proyecto, este ámbito debe ser conciso y preciso, puesto que se define el alcance y no se pretende englobar más de lo que corresponde.

En tal virtud se declara que este SGSI será implementando en los procesos que involucran los sistemas de información y los usuarios asociados a los mismos, partiendo principalmente del centro de datos y el departamento de TICS, en estos sistemas se realizan los principales procesos objetos del funcionamiento del negocio e incluye a otros secundarios o de infraestructura, ambos de manera general son los que hacen

posible la gestión de información referente a estudiantes-padres de familia (clientes) y empleados de la institución.

Los equipos de infraestructura de red, servidores, sistemas de video vigilancia, y demás activos informáticos no directamente considerados críticos para la institución están incluidos en el propósito del presente trabajo, así como también el aseguramiento lógico y físico de los equipos tecnológicos.

En la siguiente gráfica se representan los activos inmiscuidos en el SGSI, descritos anteriormente de manera general y precisados en apartados posteriores:

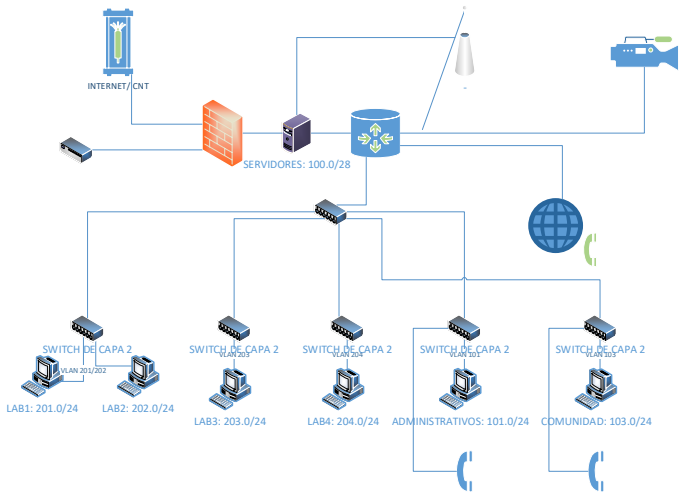

Ilustración 3: Diagrama de red de activos informáticos de la UESMA

La consumación de este proyecto entre tantos beneficios para la institución permitirá:

- ✓ Identificar vulnerabilidades y poder administrarlas.
- ✓ Planear la gestión de incidentes y continuidad de negocio.
- ✓ Implementar medidas de seguridad de la información que minimicen la perdida de la misma.
- ✓ Amplificar el prestigio y la reputación de la institución.

1.4 ANÁLISIS DIFERENCIAL

Según la norma ISO 27001 no es relevante un análisis de la situación inicial previo a la ejecución de un plan director de seguridad, pero otros modelos como el de Capacidad y Madurez que permite evaluar procesos de una organización, establece que es necesario conocer la situación actual, y se debe tener en cuenta que al usarse la metodología cíclica PDCA se debe conocer donde se inicia y de qué manera se concluye un ciclo, así se tendrá presente la efectividad de los procesos usados. La misma ISO

propone un catálogo de 114 controles disponibles para ser aplicados en una empresa y plantea que cada organización adopte los que considere necesarios según los procesos que se consumen en la misma.

A continuación, se presenta la tabla 1 que muestra las métricas a usarse para determinar el nivel en el que se encuentran los requerimientos y controles en la Unidad Educativa Salesiana María Auxiliadora.

Estado	Significado
? Desconocido	No ha sido verificado
Inexistente	No se lleva a cabo el control de seguridad en los sistemas de información.
Inicial	Las salvaguardas existen, pero no se gestionan, no existe un proceso formal para realizarlas. Su éxito depende de la buena suerte y de tener personal de la alta calidad.
Repetible	La medida de seguridad se realiza de un modo totalmente informal (con procedimientos propios, informales). La responsabilidad es individual. No hay formación.
Definido	El control se aplica conforme a un procedimiento documentado, pero no ha sido aprobado ni por el Responsable de Seguridad ni el Comité de Dirección.
Administrado	El control se lleva a cabo de acuerdo a un procedimiento documentado, aprobado y formalizado.
Optimizado	El control se aplica de acuerdo a un procedimiento documentado, aprobado y formalizado, y su eficacia se mide periódicamente mediante indicadores.
No aplicable	A fin de certificar un SGSI, todos los requerimientos principales de ISO/IEC 27001 son obligatorios. De otro modo, pueden ser ignorados por la Administración.

Tabla 1: Nomenclatura del estado de los procesos y/o controles.

Conociendo los posibles estados que pueden ser asignados a los diferentes procesos que debería realizar la institución para poder garantizar la seguridad de los servicios de información es presentada de manera consecutiva la tabla de los 27 requerimientos del Sistema Gestor de Seguridad de la Información provisto por la ISO 27001.

Sección	Requerimientos ISO 27001	Estado
4	**Contexto de la organización**	
4.1	**Comprensión de la organización y de su contexto**	
4.1	Determinar los objetivos del SGSI de la organización y cualquier problema que pueda afectar su eficacia	Inexistente
4.2	**Comprensión de las necesidades y expectativas de las partes interesadas**	
4.2 (a)	Identificar las partes interesadas incluyendo leyes aplicables, regulaciones, contratos, etc.	Repetible
4.2 (b)	Determinar los requerimientos y obligaciones relevantes de seguridad de la información	Repetible
4.3	**Determinación del alcance del SGSI**	
4.3	Determinar y documentar el alcance del SGSI	Inexistente
4.4	**SGSI**	
4.4	Establecer, implementar, mantener y mejorar de forma continua el SGSI acorde al estándar	Inexistente
5	**Liderazgo**	
5.1	**Liderazgo y compromiso**	
5.1	La administración debe demostrar liderazgo y compromiso por el SGSI	Inexistente
5.2	**Política**	
5.2	Documentar la Política de Seguridad de la Información	Inexistente
5.3	**Roles, responsabilidades y autoridades en la organización**	
5.3	Asignar y comunicar los roles y responsabilidades de seguridad de la información	Repetible
6	**Planificación**	
6.1	**Acciones para tratar los riesgos y oportunidades**	
6.1.1	Diseñar el SGSI para satisfacer los requerimientos, tratando riesgos e identificando oportunidades	Inexistente
6.1.2	Definir e implementar un proceso de análisis de riesgos de seguridad de la información	Inicial

6.1.3	Documentar e implementar un proceso de tratamiento de riesgos de seguridad de la información	Inicial
6.2	**Objetivos de seguridad de la información y planificación para su consecución**	
6.2	Establecer y documentar los planes y objetivos de la seguridad de la información	Inicial
7	**Soporte**	
7.1	**Recursos**	
7.1	Determinar y asignar los recursos necesarios para el SGSI	Inexistente
7.2	**Competencia**	
7.2	Determinar, documentar hacer disponibles las competencias necesarias	Repetible
7.3	**Concienciación**	
7.3	Implementar un programa de concienciación de seguridad	Repetible
7.4	**Comunicación**	
7.4	Determinar la necesidades de comunicación internas y externas relacionadas al SGSI	Inicial
7.5	**Información documentada**	
7.5.1	Proveer documentación requerida por el estándar más la requerida por la organización	Inexistente
7.5.2	Proveer un título, autor, formato consistente, revisión y aprobación a los documentos	Inexistente
7.5.3	Mantener un control adecuado de la documentación	Inicial
8	**Operación**	
8.1	**Planificación y control operacional**	
8.1	Planificar, implementar, controlar y documentar el proceso de gestión de riesgos del SGSI (Tratamiento de riesgos)	Inexistente
8.2	**Apreciación de los riesgos de seguridad de la información**	
8.2	Evaluar y documentar los riesgos de seguridad regularmente y cuando hay cambios	Inicial
8.3	**Tratamiento de los riesgos de seguridad de la información**	
8.3	Implementar un plan de tratamiento de riesgos y documentar los resultados	Inicial
9	**Evaluación del desempeño**	

9.1	**Seguimiento, medición, análisis y evaluación**	
9.1	Realizar un seguimiento, medición, análisis y evaluación del SGSI y los controles	Inicial
9.2	**Auditoría interna**	
9.2	Planificar y realizar una auditoria interna del SGSI	Inexistente
9.3	**Revisión por la dirección**	
9.3	La administración realiza una revisión periódica del SGSI	Inexistente
10	**Mejora**	
10.1	**No conformidad y acciones correctivas**	
10.1	Identificar, arreglar y reaccionar ante no conformidades para evitar su recurrencia documentando todas las acciones	Inexistente
10.2	**Mejora continua**	
10.2	Mejora continua del SGSI	Inexistente

Tabla 2: Requerimientos ISO 27001

A continuación, es presentada la tabla 2 con los controles establecidos en la ISO 27001 para un SGSI, esta se basa en los procesos que actualmente realiza la institución en marco a la seguridad de la información y consta de 114 dominios.

Sección	Controles de Seguridad de la Información	Estado	Comentarios
A5	**Políticas de seguridad de la información**		
A5.1	**Directrices de gestión de la seguridad de la información**		

A5.1.1	Políticas para la seguridad de la información	Inicial	La institución no cuenta con medidas documentadas de seguridad de la información
A5.1.2	Revisión de las políticas para la seguridad de la información	Inicial	
A6	**Organización de la seguridad de la información**		
A6.1	**Organización interna**		
A6.1.1	Roles y responsabilidades en seguridad de la información	Repetible	Aunque no existe un tratamiento de la seguridad de la información general, los responsables del departamento informático realizan configuraciones los sistemas para salvaguardar los mismos y en ciertos proyectos relacionados con el área. Las autoridades no están involucradas con una planificación
A6.1.2	Segregación de tareas	Inexistente	
A6.1.3	Contacto con las autoridades	Inexistente	

A6.1.4	Contacto con grupos de interés especial	Inexistente	
A6.1.5	Seguridad de la información en la gestión de proyectos	Inicial	
A6.2	**Los dispositivos móviles y el teletrabajo**		
A6.2.1	Política de dispositivos móviles	Definido	Es posible vincular los dispositivos móviles personales a la red wifi institucional, para el personal administrativo se encuentra disponible una línea VOIP móvil en sus smartphones.
A6.2.2	Teletrabajo	No aplicable	No se realiza teletrabajo
A7	**Seguridad relativa a los recursos humanos**		
A7.1	**Antes del empleo**		
A7.1.1	Investigación de antecedentes	Inicial	GTH se basa en lo expuesto en las hojas de vida y comentarios si los comentarios de otros empleados si los existiesen
A7.1.2	Términos y condiciones del empleo	Inicial	El contrato de trabajo simplemente se detallan las funciones a realizar y no toma en cuenta todos los roles de la institución, cuando es asignada una función diferente a la de docente, contador, secretaria o dece solo se expone oralmente las responsabilidades

A7.2	**Durante el empleo**		
A7.2.1	Responsabilidades de gestión	Repetible	De manera empírica se lo realiza con ciertos grupos de empleados en modo de conversación
A7.2.2	Concienciación, educación y capacitación en seguridad de la información	Inicial	
A7.2.3	Proceso disciplinario	Repetible	No se aplica a todos los empleados puesto que no hay una política.
A7.3	**Finalización del empleo o cambio en el puesto de trabajo**		
A7.3.1	Responsabilidades ante la finalización o cambio	Inicial	No se definen acuerdos en la finalización de contratos con la institución
A8	**Gestión de activos**		
A8.1	**Responsabilidad sobre los activos**		

A8.1.1	Inventario de activos	Administrado	Existe un sistema que realiza la gestión de los activos de TI y permita asignar ubicación y responsables, aunque no se ha actualizado n los últimos 3 años
A8.1.2	Propiedad de los activos	Definido	
A8.1.3	Uso aceptable de los activos	Definido	
A8.1.4	Devolución de activos	Definido	Según la ley y código de convivencia se debe realizar pero en ocasiones no se aplica
A8.2	**Clasificación de la información**		
A8.2.1	Clasificación de la información	Inicial	No hay políticas relacionada con la clasificación de la información, ciertos SI son clasificados pero no hay un procedimiento definido
A8.2.2	Etiquetado de la información	Inicial	

A8.2.3	Manipulado de la información	Inicial	
A8.3	**Manipulación de los soportes**		
A8.3.1	Gestión de soportes extraíbles	Inicial	No existe un proceso definido para la gestión de medios extraíbles, en ocasiones se realizan acciones sobre estos dependiendo el uso previo de los mismos
A8.3.2	Eliminación de soportes	Repetible	
A8.3.3	Soportes físicos en tránsito	No aplicable	No se realiza transportación de dispositivos
A9	**Control de acceso**		
A9.1	**Requisitos de negocio para el control de acceso**		
A9.1.1	Política de control de acceso	Inicial	No existe una política definida pero en ciertos roles se realiza el control
A9.1.2	Acceso a las redes y a los servicios de red	Repetible	Las políticas son manifestadas de manera verbal pero no existen controles para identificar el mal uso de los servicios de red.
A9.2	**Gestión de acceso de usuario**		

A9.2.1	Registro y baja de usuario	Inicial	No existe una política clara definida pero debe ser un proceso habitual en toda la empresa, se pudo constatar que existen usuarios en los sistemas de información que cesaron funciones hace mas de dos años
A9.2.2	Provisión de acceso de usuario	Inicial	Solamente es aplicado sin documentación en el departamento de contabilidad
A9.2.3	Gestión de privilegios de acceso	Inicial	Solamente es aplicado sin documentación en el departamento de contabilidad
A9.2.4	Gestión de la información secreta de autenticación de los usuarios	Inicial	Se realizan sugerencias de contraseñas pero existe un proceso para comprobar la aplicación
A9.2.5	Revisión de los derechos de acceso de usuario	Repetible	Se realiza de manera empírica pero no periódico, no es aplicada a todos los usuarios
A9.2.6	Retirada o reasignación de los derechos de acceso	Inicial	No existe documentación que registre este proceso pero de manera verbal se han fijado términos en ciertas ocasiones
A9.3	**Responsabilidades del usuario**		
A9.3.1	Uso de la información secreta de autenticación	Inicial	No existe proceso de aseguramiento de estos datos
A9.4	**Control de acceso a sistemas y aplicaciones**		

A9.4.1	Restricción del acceso a la información	Repetible	No es un proceso definido pero se realiza en ciertas ocasiones
A9.4.2	Procedimientos seguros de inicio de sesión	Inicial	Se realizan sugerencias de contraseñas pero existe un proceso centralizada para poder comprobar
A9.4.3	Sistema de gestión de contraseñas	Inicial	
A9.4.4	Uso de utilidades con privilegios del sistema	Repetible	El departamento de TI es el responsable de la administración pero no se realiza un control sobre estos
A9.4.5	Control de acceso al código fuente de los programas	Repetible	No se realiza desarrollo de software en la institución
A10	**Criptografía**		
A10.1	**Controles criptográficos**		
A10.1.1	Política de uso de los controles criptográficos	No aplicable	No manejan información que deba estar protegida a este nivel

A10.1.2	Gestión de claves	No aplicable	
A11	**Seguridad física y del entorno**		
A11.1	**Áreas seguras**		
A11.1.1	Perímetro de seguridad física	Administrado	La infraestructura física es uno de los puntos fuertes referentes a la seguridad de los equipos y sistemas TI por los distintos lineamientos que debe cumplir como institución educativa aunque existes equipos de cómputo no muy seguros de acceso no autorizado en relación a otros empleados
A11.1.2	Controles físicos de entrada	Definido	
A11.1.3	Seguridad de oficinas, despachos y recursos	Definido	
A11.1.4	Protección contra las amenazas externas y ambientales	Administrado	

A11.1.5	El trabajo en áreas seguras	Administrado	
A11.1.6	Áreas de carga y descarga	Definido	
A11.2	**Seguridad de los equipos**		
A11.2.1	Emplazamiento y protección de equipos	Definido	El lugar es seguro frente a adversidades del entorno pero para acceder solo necesita una llave que es fácilmente adquirible
A11.2.2	Instalaciones de suministro	Optimizado	Existen baterías de energía eléctrica instaladas después de un estudio de necesidad
A11.2.3	Seguridad del cableado	Definido	Se han realizado las instalaciones bajo parámetros de cableado estructurado, a excepción de nuevas instalaciones realizadas en el último año
A11.2.4	Mantenimiento de los equipos	Definido	Existen fechas y responsables calificados para el mantenimiento de equipos pero no se lleva un control o informe del proceso

A11.2.5	Retirada de materiales propiedad de la empresa	Inicial	No hay políticas que definan la responsabilidad o autorización para extraer un equipo de la institución
A11.2.6	Seguridad de los equipos fuera de las instalaciones	Inicial	
A11.2.7	Reutilización o eliminación segura de equipos	Definido	Cuando los equipos de computo son asignados a nuevos responsables se procede a formatear.
A11.2.8	Equipo de usuario desatendido	Repetible	Se realiza a voluntad de los usuarios y en ocasiones por la configuración de fábrica de los sistemas operativos
A11.2.9	Política de puesto de trabajo despejado y pantalla limpia	Repetible	
A12	**Seguridad de las operaciones**		
A12.1	**Procedimientos y responsabilidades operacionales**		

A12.1.1	Documentación de procedimientos operacionales	Repetible	No existen políticas definidas para estos procesos, en ocasiones se realiza por voluntad de los responsables de TI
A12.1.2	Gestión de cambios	Inicial	
A12.1.3	Gestión de capacidades	Inicial	
A12.1.4	Separación de los recursos de desarrollo, prueba y operación	No aplicable	No se realiza desarrollo de software en la institución
A12.2	**Protección contra el software malicioso (malware)**		

A12.2.1	Controles contra el código malicioso	Inicial	Solo en equipos de computo se procura mantener actualizado el antivirus propio del sistema operativo, el resto se improvisa al presentarse el inconveniente
A12.3	**Copias de seguridad**		
A12.3.1	Copias de seguridad de la información	Definido	Se tiene planificado un calendario de copias de seguridad y respaldos pero en ocasiones no se cumple
A12.4	**Registros y supervisión**		
A12.4.1	Registro de eventos	Inicial	Se realizan ciertos procesos de manera empírica y no son documentados

A12.4.2	Protección de la información del registro	Inicial	
A12.4.3	Registros de administración y operación	Inicial	
A12.4.4	Sincronización del reloj	Inicial	
A12.5	**Control del software en explotación**		
A12.5.1	Instalación del software en explotación	Definido	Se procura que el software cumpla con el propósito y son usadas las licencias del sistema operativo windows y para el paquete de oficina de microsoft
A12.6	**Gestión de la vulnerabilidad técnica**		
A12.6.1	Gestión de las vulnerabilidades técnicas	Repetible	Cuando se presenta alguna inconsistencia se toman acciones no documentadas

A12.6.2	Restricción en la instalación de software	Repetible	De manera verbal se manifiesta a los usuarios la limitación frente a la instalación de software ajeno a las funciones pero no existe un control de aquello
A12.7	**Consideraciones sobre la auditoria de sistemas de información**		
A12.7.1	Controles de auditoría de sistemas de información	Inexistente	No se realizan auditorias de SI
A13	**Seguridad de las comunicaciones**		
A13.1	**Gestión de la seguridad de las redes**		
A13.1.1	Controles de red	Definido	Se han realizado ciertas configuraciones no documentadas y frente a inconvenientes presentados solo se resuelven en ocasiones parcialmente, algunos elementos están disponibles pero no son usados, la división de redes no se ha realizado de manera eficaz y eficiente
A13.1.2	Seguridad de los servicios de red	Administrado	
A13.1.3	Segregación en redes	Definido	
A13.2	**Intercambio de información**		

A13.2.1	Políticas y procedimientos de intercambio de información	Inicial	No existen procesos definidos del envió recepción de información, se aplican controles empíricos.
A13.2.2	Acuerdos de intercambio de información	Inicial	
A13.2.3	Mensajería electrónica	Inexistente	
A13.2.4	Acuerdos de confidencialidad o no revelación	Inexistente	
A14	**Adquisición, desarrollo y mantenimiento de los sistemas de información**		
A14.1	**Requisitos de seguridad en los sistemas de información**		
A14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	Inicial	Existe una planificación no formal que no se cumple rigurosamente, se realiza en ocasiones de manera empírica

A14.1.2	Asegurar los servicios de aplicaciones en redes públicas	Inicial	
A14.1.3	Protección de las transacciones de servicios de aplicaciones	Repetible	
A14.2	**Seguridad en el desarrollo y en los procesos de soporte**		
A14.2.1	Política de desarrollo seguro	No aplicable	No se realiza desarrollo de software en la institución
A14.2.2	Procedimiento de control de cambios en sistemas	Definido	En el contrato realizado para la adquisición de un software se definiera procesos para realizar adecuaciones en el mismo
A14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	Definido	Se realiza pero no hay un registro de las actividades realizadas
A14.2.4	Restricciones a los cambios en los paquetes de software	Definido	
A14.2.5	Principios de ingeniería de sistemas seguros	No aplicable	No se realiza desarrollo de software en la institución

A14.2.6	Entorno de desarrollo seguro	No aplicable	
A14.2.7	Externalización del desarrollo de software	Administrado	Se realiza contratos con entidades externas para el desarrollo de software y estos están bajo contratos en los cuales se define la función y alcance de los sistemas desarrollados
A14.2.8	Pruebas funcionales de seguridad de sistemas	Administrado	
A14.2.9	Pruebas de aceptación de sistemas	Administrado	
A14.3	**Datos de prueba**		
A14.3.1	Protección de los datos de prueba	Inicial	Se realizan pruebas pero simplemente son borradas posteriormente de la base de datos por el proveedor
A15	**Relación con proveedores**		
A15.1	**Seguridad en las relaciones con proveedores**		

A15.1.1	Política de seguridad de la información en las relaciones con los proveedores	Administrado	Se realiza contratos con entidades externas para el desarrollo de software y estos están bajo contratos en los cuales se define la función y alcance de los sistemas desarrollados
A15.1.2	Requisitos de seguridad en contratos con terceros	Administrado	
A15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	Inicial	No hay procesos de comprobación de la seguridad de la información en los sistemas desarrollados por terceros
A15.2	**Gestión de la provisión de servicios del proveedor**		
A15.2.1	Control y revisión de la provisión de servicios del proveedor	Administrado	Existe una buena comunicación con las empresas responsable del desarrollo de sistemas de información y se establece en los contratos apertura a modificaciones
A15.2.2	Gestión de cambios en la provisión del servicio del proveedor	Definido	
A16	**Gestión de incidentes de seguridad de la información**		

A16.1	Gestión de incidentes de seguridad de la información y mejoras		
A16.1.1	Responsabilidades y procedimientos	Repetible	La gestión de incidentes se realiza de manera empírica y una vez solucionado el inconveniente no son tomadas medidas para evitar problemas futuros ni es documentado el proceso tomado para resolverlo ni el factor causante.
A16.1.2	Notificación de los eventos de seguridad de la información	Repetible	
A16.1.3	Notificación de puntos débiles de la seguridad	Inicial	
A16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	Inicial	
A16.1.5	Respuesta a incidentes de seguridad de la información	Inicial	
A16.1.6	Aprendizaje de los incidentes de seguridad de la información	Repetible	
A16.1.7	Recopilación de evidencias	Inicial	

A17	**Aspectos de seguridad de la información para la gestión de la continuidad de negocio**		
A17.1	**Continuidad de la seguridad de la información**		
A17.1.1	Planificación de la continuidad de la seguridad de la información	Repetible	Los responsables de TI toma ciertas medidas de seguridad pero no existe una planificación de la misma
A17.1.2	Implementar la continuidad de la seguridad de la información	Repetible	
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Repetible	
A17.2	**Redundancias**		
A17.2.1	Disponibilidad de los recursos de tratamiento de la información	Inicial	En caso de desastres en los sistemas de información únicamente el sistema contable tiene respaldo de la información pero no de configuraciones
A18	**Cumplimiento**		
A18.1	**Cumplimiento de los requisitos legales y contractuales**		
A18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Repetible	Las políticas son tomadas por los responsables de TI pero no están documentadas

A18.1.2	Derechos de Propiedad Intelectual (DPI)	Definido	Se procura que el software propietario tenga licencia pero no se realiza el control necesario para evitar que esto suceda en todos los dispositivos
A18.1.3	Protección de los registros de la organización	Inicial	No existe una política ni documentos de procedimientos relacionados a la protección de información personal, pero los responsables de estos de manera autónoma emplean mecanismos de protección
A18.1.4	Protección y privacidad de la información de carácter personal	Inicial	
A18.1.5	Regulación de los controles criptográficos	Inicial	
A18.2	**Revisiones de la seguridad de la información**		
A18.2.1	Revisión independiente de la seguridad de la información	Inicial	No está definida la importancia de los activos de información y no se realiza auditoria sobre estos. En ocasiones se realizan proceso para probar funcionamiento por parte de los responsable de TI
A18.2.2	Cumplimiento de las políticas y normas de seguridad	Repetible	
A18.2.3	Comprobación del cumplimiento técnico	Repetible	

Tabla 3: Controles de Anexo A en la UESMA.

1.4.1 CONCLUSIÓN

La tabla a continuación muestra el porcentaje de cada métrica con respecto a los requisitos que debiera cumplir la UESMA y los controles que actualmente se aplican relacionados al Sistema Gestor de Seguridad de la Información.

Estado	Significado	Proporción de requerimientos SGSI	Proporción de Controles de Seguridad de la Información
? Desconocido	No ha sido verificado	0%	0%
Inexistente	No se lleva a cabo el control de seguridad en los sistemas de información.	52%	5%
Inicial	Las salvaguardas existen, pero no se gestionan, no existe un proceso formal para realizarlas. Su éxito depende de la buena suerte y de tener personal de la alta calidad.	30%	39%
Repetible	La medida de seguridad se realiza de un modo totalmente informal (con procedimientos propios, informales). La responsabilidad es individual. No hay formación.	19%	21%
Definido	El control se aplica conforme a un procedimiento documentado, pero no ha sido aprobado ni por el Responsable de Seguridad ni el Comité de Dirección.	0%	18%
Administrado	El control se lleva a cabo de acuerdo a un procedimiento documentado, aprobado y formalizado.	0%	10%
Optimizado	El control se aplica de acuerdo a un procedimiento documentado, aprobado y formalizado, y su eficacia se mide periódicamente mediante indicadores.	0%	1%
No aplicable	A fin de certificar un SGSI, todos los requerimientos principales de ISO/IEC 27001 son obligatorios. De otro modo, pueden ser ignorados por la Administración.	0%	7%
	Total	100%	100%

Tabla 4: Resultado por dominios de análisis referencial.

Como resultado se obtiene que de los requisitos obligatorios que establece la ISO 27001 para un Sistema Gestor de Seguridad de la Información la UESMA tiene un 52% obligaciones inexistentes, es decir no se aplican 14 de los 27 controles, en estado inicial hay un total de 8 elementos, lo cual equivale al 30% de requisitos que no se gestionan ni tienen un proceso formalmente documentado, finalmente en estado repetible tiene un 18% o 5 compendios, estos son los que se realizan de manera totalmente informal y de manera empírica por parte de alguno de los responsables sobre los sistemas, generalmente parte de los responsables del departamento de TI.

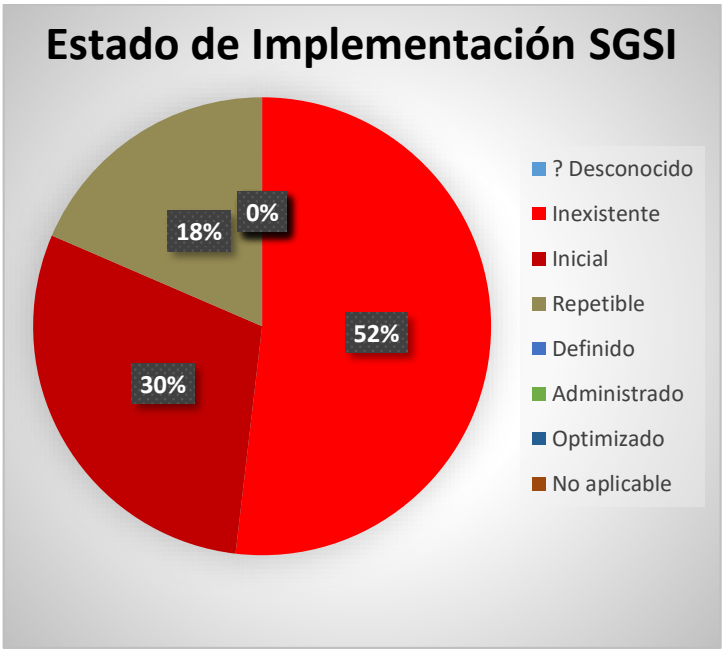

Ilustración 4: Resultado de requisitos SGSI que cumple la UESMA.

Referente a los 114 controles del Anexo A se conoce que el 5% de estos fueron descritos como inexistentes, es decir 6 de los procesos no se realizan, en estado inicial se ubican 44 controles que equivalen al 39% del total, es decir se ha planteado realizar estos controles, pero no hay evidencia de su ejecución, con el 21% que equivale a 24 controles situados en la métrica de repetible, es decir se realizan por voluntad de usuarios o responsables de las TICs, etiquetados como definidos hay un 18% de los registros, es decir 20 de estos están documentados pero en vista que no existe un responsable de la seguridad no está aprobado ni forma parte de una política definida, estos se realizan parcialmente. Métricamente aceptables se establece con 10% proporcional a 8 controles administrados, mismos que se cumplen mediante un procedimiento documento que ha sido planteado como política y es reconocido por el departamento de TI y las autoridades de la institución pese a que no hay un SGSI, finalmente resalta un control como

optimizado, “Instalaciones de suministros” es el punto más fuerte de la institución puesto que se cumplió con un rigurosa análisis y la inversión necesaria para la adecuación del sistema eléctrico con respaldo de energía, lo cual ha dado muy buenos resultados frente al inconveniente que acarrea en la zona referente a cortes de energía eléctrica, dejando 8 controles como no aplicables, estos en su mayoría relacionados con el desarrollo de software dentro de la institución.

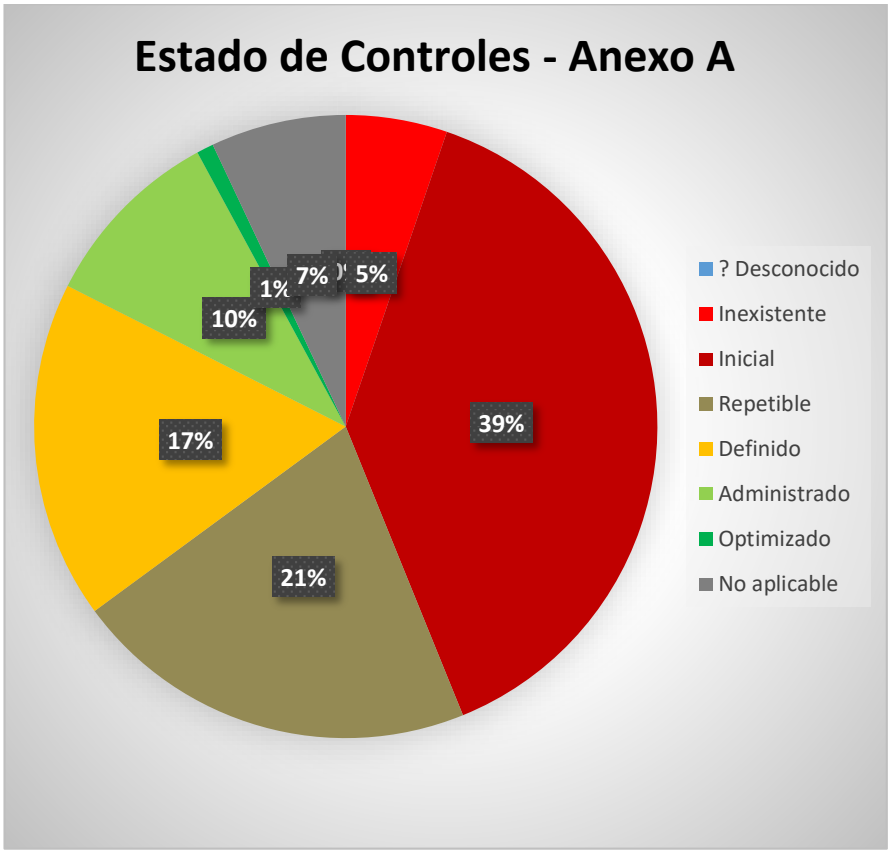

Ilustración 5: Resultados de los controles Anexo A en la UESMA

Frente a estos resultados se puede deducir que el SGSI en esta institución se encuentra en un nivel considerablemente inmaduro de implementación.

FASE 2: SISTEMA DE GESTIÓN DOCUMENTAL

2.1 INTRODUCCIÓN

Todos los Sistemas de Gestión se apoyan en un cuerpo documental para el cumplimiento normativo. Esto significa que en nuestro Sistema de Gestión de Seguridad de la Información tendremos que tener una serie de documentos, los cuales vienen establecidos en la propia norma ISO/IEC 27001

2.2 ESQUEMA DOCUMENTAL

Los sistemas de gestión deben estar basados en un sistema de gestión documental, este proyecto al ser un Sistema de Gestión de Seguridad de la Información no es la excepción, y la ISO 27001 enfatiza la necesidad de documentos habilitantes para certificar un sistema, que, aunque este proyecto no pretende que se pase la certificación internacional ISO si es importante que cumpla con las pautas en estos estándares descritos.

La Unidad Educativa Salesiana María Auxiliadora no evidencia cumplir con esta normativa al no poseer ningún documento referente al marco conceptual del SGSI que se pretende implementar, a excepción de decisiones propias de varios usuarios, en gran parte los responsables de las TIC, por lo tanto, en esta fase se aspira desarrollar la información necesaria según lo establece el estándar ISO asociado a la SI, misma que se presenta en el gráfico a continuación:

Ilustración 6: Políticas de seguridad de la información

2.3 POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

2.3.1 Prólogo

La UESMA tiene como misión los procesos de enseñanza aprendizaje, pero existen algunos sistemas de información que facilitan la gestión desde el momento que ingresa el estudiante hasta que obtiene su título de bachiller o por el contrario continua sus estudios en otra institución, estos activos deben tener un reglamento de uso y que se valoren las medidas de seguridad necesarias para resguardar la información y procesos consumados en estos.

Estas medidas de seguridad son un continuo proceso de actualización y adaptación aplicado a las bases del negocio, dirigido a todo ambiente físico, lógico, humano y técnico asociado a los sistemas y activos de información que se pretende asegurar en el presente proyecto.

2.3.2 Marco legal y normativo

Las políticas de seguridad serán desarrolladas entorno a lo descrito en las normativas, reglamentos y leyes descritas a continuación:

- ✓ ISO/IEC 27001:2013 e ISO/IEC 27002:2013.
- ✓ Constitución de la república del Ecuador.
- ✓ Ley orgánica de comunicación del Ecuador.
- ✓ Ley orgánica de transparencia y acceso a la información.
- ✓ Código orgánico penal del Ecuador
- ✓ Ley de comercio electrónico, firmas electrónicas y mensajes de datos.
- ✓ Reglamento general a la Ley Orgánica del Servicio Público.
- ✓ Acuerdo No 166, Esquema Gubernamental de Seguridad de la Información EGSI.

2.3.3 Responsables

Directo: Coordinador del departamento de TICS, responsable de elaborar, evaluar y actualizar la presente política.

Todo el personal: Cumplen la función de analizar, aprobar y cumplir con las políticas de seguridad de la información.

2.3.4 Principios

- ✓ Confidencialidad: La información debe estar únicamente disponible para los involucrados o personas autorizadas para acceder a las mismas
- ✓ Integridad: Se debe garantizar que la información es veraz y autentica, no ha sufrido manipulación y se presenta tal y como es.
- ✓ Disponibilidad: La información debe estar disponible cuando el usuario/propietario de la misma necesite disponer de la misma.

- ✓ Gestión del riesgo: Debe ser minimizados a niveles aceptables los incidentes que pudiesen darse.
- ✓ Mejora continua: Los controles, medidas de seguridad y todos los documentos resultantes de este proceso deben ser evaluados y actualizados periódicamente.
- ✓ Ética: Los involucrados con la información deben respetar los derechos e intereses de los demás.
- ✓ Concientización: Es necesario plantear uno o varios horarios de inducción en los cuales participen todas las personas relacionadas con la institución y los activos de información.

2.3.5 Directrices de seguridad

- ✓ Todo el personal interno y externo de la institución debe firmar un documento que evidencie que conoce las políticas de seguridad de la información.
- ✓ Los activos de información asignados acordes a cada rol deben ser de uso exclusivo para fines alineados con los objetivos y procesos institucionales.
- ✓ Los activos descritos en el literal anterior deben ser entregados al Jefe de Bodega previo al cese de funciones y el departamento informático evaluara el funcionamiento y uso del mismo.
- ✓ Los empleados de la institución deben firmar un acuerdo de confidencialidad y no divulgación; de no cumplirse puede ser sancionado como lo estipulan los artículos 178, 190 y 230 del código orgánico penal del Ecuador.
- ✓ A cada usuario según su rol les serán asignadas credenciales de acceso a los equipos de cómputo, este será el único custodio de estos y es directamente responsable de los hechos que se realizasen desde este perfil de usuario.
- ✓ Todo el personal de la institución seguirá las directrices de clasificación de la información.
- ✓ Se establece como medio de intercambio de información el correo electrónico institucional.
- ✓ Cada usuario es responsable de la cuenta de correo electrónico asignada a su cargo y por lo tanto del contenido recibido y enviado.
- ✓ Los sistemas de información y activos de redes deben cumplir aspectos de seguridad señalados en estándares nacionales e internacionales.
- ✓ El responsable de la seguridad de la información deberá gestionar los incidentes y garantizar la continuidad de negocio apoyado en el SGSI.
- ✓ Todo el personal debe recibir a través de los medios de comunicación oficiales las instrucciones y documentación necesaria para prevalecer la seguridad de la información según el rol asignado en el contrato y sus funciones.
- ✓ Se debe garantizar la privacidad de los datos de todos los clientes de la institución alojados en los sistemas de información.
- ✓ Los clientes son los responsables de otorgar información autentica y de las credenciales de acceso al sistema académico ProsoftEdu, así como de las acciones que se realizasen con el mismo.
- ✓ Todo el personal que detectase algún inconveniente en los sistemas de información debe comunicar al responsable a través de los medios oficiales de manera inmediata.

Nota: La política de seguridad de la información mencionada debe ser aplicada por todo el personal docente, administrativo y de servicio de la institución, y en los puntos que se

consideran a los clientes (estudiantes y padres de familia) debe ser acatada en su totalidad, estas deben ser publicadas en todos los medios de comunicación posibles.

2.4 PROCEDIMIENTO DE AUDITORIA INTERNA

2.4.1 Prólogo

Según Tamayo Alonso, la auditoría de sistemas de información o auditoria de seguridad informática es el proceso de análisis y gestión de sistemas informáticos por parte de profesionales y tiene como objetivo identificar, enlistar y describir las vulnerabilidades que pudiesen encontrarse en una revisión. Estas vulnerabilidades pueden ser lógica, físicas o procesos sobre los sistemas de información, de manera general permite conocer la situación exacta de los sistemas de información en cuanto a protección, control y medidas de seguridad.

2.4.2 Objetivo

Evaluar los aspectos físicos, lógicos y procedimentales relacionados a los activos tecnológicos de la institución con el fin de conocer y mejorar la seguridad de los sistemas de información para poder garantizar lo continuidad de los procesos arraigados a los objetivos del negocio basado en el SGSI sustentado en las normas ISO/IEC 27001:2013 e ISO/IEC 27002:2013.

2.4.3 Responsables

- ✓ Coordinador del departamento TIC.
- ✓ Directivos.
- ✓ Coordinadores departamentales involucrados con activos de información.

2.4.4 Proceso de auditoria

Fase 1: Exploración

En esta fase se pretende conocer la situación actual de la institución, identificar los activos de información contemplados en el alcance del SGSI y los responsables de cada equipo/sistema informático. De haberse realizado auditorias anteriores serán revisadas en esta etapa.

Fase 2: Planeamiento.

Ya teniendo un punto de partida se procede a organizar el proceso de auditoría, en esta etapa se establecen los horarios en los cuales van a ser analizados cada uno de los sistemas de información, los test que se realizarán y la documentación que debe constar en posesión de los responsables de cada uno de los activos. Los responsables deben reunirse e informar a todos los implicados el plan de auditoria.

Fase 3: Ejecución

Se procede a ejecutar lo planeado en la fase anterior como trabajo de campo in situ, es decir se analizará cada sistema y activo de información en presencia del responsable del activo, se solicitarán documentos que evidencien procesos acordes a la seguridad de la información y el responsable del activo debe responder todas las cuestiones que se le planteen, estos detalles permitirán llenar la matriz que se detalla en la tabla 2. Esta es la fase más extensa del proceso de auditoría.

Fase 4: Informe.

Al finalizar el trabajo de campo el equipo auditor tendrá un periodo de no más de 24 horas para consolidar y presentar los detalles de los resultados de la auditoria en presencia de los directivos de la institución y los responsables de cada activo de información auditado. Aquí también será propuesto un plan de mejora y se establecerá en conjunto fechas para concretarlos.

Fase 5: Seguimiento

Según lo acordado en el informe con los planes de mejora los responsables de la auditoria deben mantener reuniones periódicas para comprobar la aplicación de los correctivos descritos en la fase anterior.

La siguiente tabla presenta una planificación de los controles a desarrollarse y auditarse en los siguientes tres años, con el fin de realizar una aplicación del SGSI progresiva, dando prioridad a aquellos controles que se consideren de carácter crítico y relevantes en el contorno de la seguridad de la información de la UESMA de acuerdo a la importancia de sus procesos.

Sección	Controles de Seguridad de la Información	Periodicidad		
		1ER AÑO	2DO AÑO	3ER AÑO
A5	**Políticas de seguridad de la información**			
A5.1	**Directrices de gestión de la seguridad de la información**			
A5.1.1	Políticas para la seguridad de la información	X		
A5.1.2	Revisión de las políticas para la seguridad de la información	X		

A6	**Organización de la seguridad de la información**			
A6.1	**Organización interna**			
A6.1.1	Roles y responsabilidades en seguridad de la información	X		
A6.1.2	Segregación de tareas	X		
A6.1.3	Contacto con las autoridades	X		
A6.1.4	Contacto con grupos de interés especial	X		
A6.1.5	Seguridad de la información en la gestión de proyectos	X		
A6.2	**Los dispositivos móviles y el teletrabajo**			
A6.2.1	Política de dispositivos móviles			X
A6.2.2	Teletrabajo			X
A7	**Seguridad relativa a los recursos humanos**			
A7.1	**Antes del empleo**			
A7.1.1	Investigación de antecedentes	X		
A7.1.2	Términos y condiciones del empleo	X		
A7.2	**Durante el empleo**			
A7.2.1	Responsabilidades de gestión		X	
A7.2.2	Concienciación, educación y capacitación en seguridad de la información		X	
A7.2.3	Proceso disciplinario		X	
A7.3	**Finalización del empleo o cambio en el puesto de trabajo**			
A7.3.1	Responsabilidades ante la finalización o cambio		X	
A8	**Gestión de activos**			
A8.1	**Responsabilidad sobre los activos**			
A8.1.1	Inventario de activos		X	
A8.1.2	Propiedad de los activos		X	
A8.1.3	Uso aceptable de los activos	X		
A8.1.4	Devolución de activos			X
A8.2	**Clasificación de la información**			
A8.2.1	Clasificación de la información		X	
A8.2.2	Etiquetado de la información		X	
A8.2.3	Manipulado de la información		X	
A8.3	**Manipulación de los soportes**			
A8.3.1	Gestión de soportes extraíbles		X	
A8.3.2	Eliminación de soportes		X	
A8.3.3	Soportes físicos en tránsito		X	
A9	**Control de acceso**			
A9.1	**Requisitos de negocio para el control de acceso**			
A9.1.1	Política de control de acceso	X		
A9.1.2	Acceso a las redes y a los servicios de red	X		
A9.2	**Gestión de acceso de usuario**			
A9.2.1	Registro y baja de usuario	X		

A9.2.2	Provisión de acceso de usuario	X		
A9.2.3	Gestión de privilegios de acceso	X		
A9.2.4	Gestión de la información secreta de autenticación de los usuarios	X		
A9.2.5	Revisión de los derechos de acceso de usuario	X		
A9.2.6	Retirada o reasignación de los derechos de acceso			X
A9.3	**Responsabilidades del usuario**			
A9.3.1	Uso de la información secreta de autenticación	X		
A9.4	**Control de acceso a sistemas y aplicaciones**			
A9.4.1	Restricción del acceso a la información	X		
A9.4.2	Procedimientos seguros de inicio de sesión	X		
A9.4.3	Sistema de gestión de contraseñas		X	
A9.4.4	Uso de utilidades con privilegios del sistema		X	
A9.4.5	Control de acceso al código fuente de los programas			X
A10	**Criptografía**			
A10.1	**Controles criptográficos**			
A10.1.1	Política de uso de los controles criptográficos			X
A10.1.2	Gestión de claves			X
A11	**Seguridad física y del entorno**			
A11.1	**Áreas seguras**			
A11.1.1	Perímetro de seguridad física		X	
A11.1.2	Controles físicos de entrada		X	
A11.1.3	Seguridad de oficinas, despachos y recursos		X	
A11.1.4	Protección contra las amenazas externas y ambientales			X
A11.1.5	El trabajo en áreas seguras			X
A11.1.6	Áreas de carga y descarga			X
A11.2	**Seguridad de los equipos**			
A11.2.1	Emplazamiento y protección de equipos			X
A11.2.2	Instalaciones de suministro			X
A11.2.3	Seguridad del cableado			X
A11.2.4	Mantenimiento de los equipos		X	
A11.2.5	Retirada de materiales propiedad de la empresa		X	
A11.2.6	Seguridad de los equipos fuera de las instalaciones	X		
A11.2.7	Reutilización o eliminación segura de equipos		X	
A11.2.8	Equipo de usuario desatendido	X		
A11.2.9	Política de puesto de trabajo despejado y pantalla limpia	X		
A12	**Seguridad de las operaciones**			
A12.1	**Procedimientos y responsabilidades operacionales**			
A12.1.1	Documentación de procedimientos operacionales	X		
A12.1.2	Gestión de cambios		X	

A12.1.3	Gestión de capacidades		X	
A12.1.4	Separación de los recursos de desarrollo, prueba y operación			X
A12.2	**Protección contra el software malicioso (malware)**			
A12.2.1	Controles contra el código malicioso	X		
A12.3	**Copias de seguridad**			
A12.3.1	Copias de seguridad de la información		X	
A12.4	**Registros y supervisión**			
A12.4.1	Registro de eventos			X
A12.4.2	Protección de la información del registro			X
A12.4.3	Registros de administración y operación			X
A12.4.4	Sincronización del reloj	X		
A12.5	**Control del software en explotación**			
A12.5.1	Instalación del software en explotación		X	
A12.6	**Gestión de la vulnerabilidad técnica**			
A12.6.1	Gestión de las vulnerabilidades técnicas	X		
A12.6.2	Restricción en la instalación de software	X		
A12.7	**Consideraciones sobre la auditoria de sistemas de información**			
A12.7.1	Controles de auditoría de sistemas de información			X
A13	**Seguridad de las comunicaciones**			
A13.1	**Gestión de la seguridad de las redes**			
A13.1.1	Controles de red	X		
A13.1.2	Seguridad de los servicios de red		X	
A13.1.3	Segregación en redes		X	
A13.2	**Intercambio de información**			
A13.2.1	Políticas y procedimientos de intercambio de información	X		
A13.2.2	Acuerdos de intercambio de información		X	
A13.2.3	Mensajería electrónica		X	
A13.2.4	Acuerdos de confidencialidad o no revelación	X		
A14	**Adquisición, desarrollo y mantenimiento de los sistemas de información**			
A14.1	**Requisitos de seguridad en los sistemas de información**			
A14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	X		
A14.1.2	Asegurar los servicios de aplicaciones en redes públicas		X	
A14.1.3	Protección de las transacciones de servicios de aplicaciones		X	
A14.2	**Seguridad en el desarrollo y en los procesos de soporte**			
A14.2.1	Política de desarrollo seguro	X		
A14.2.2	Procedimiento de control de cambios en sistemas	X		
A14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo		X	
A14.2.4	Restricciones a los cambios en los paquetes de software		X	
A14.2.5	Principios de ingeniería de sistemas seguros		X	

A14.2.6	Entorno de desarrollo seguro			X
A14.2.7	Externalización del desarrollo de software			X
A14.2.8	Pruebas funcionales de seguridad de sistemas		X	
A14.2.9	Pruebas de aceptación de sistemas			X
A14.3	**Datos de prueba**			
A14.3.1	Protección de los datos de prueba		X	
A15	**Relación con proveedores**			
A15.1	**Seguridad en las relaciones con proveedores**			
A15.1.1	Política de seguridad de la información en las relaciones con los proveedores	X		
A15.1.2	Requisitos de seguridad en contratos con terceros	X		
A15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones			X
A15.2	**Gestión de la provisión de servicios del proveedor**			
A15.2.1	Control y revisión de la provisión de servicios del proveedor		X	
A15.2.2	Gestión de cambios en la provisión del servicio del proveedor		X	
A16	**Gestión de incidentes de seguridad de la información**			
A16.1	**Gestión de incidentes de seguridad de la información y mejoras**			
A16.1.1	Responsabilidades y procedimientos	X		
A16.1.2	Notificación de los eventos de seguridad de la información		X	
A16.1.3	Notificación de puntos débiles de la seguridad		X	
A16.1.4	Evaluación y decisión sobre los eventos de seguridad de información		X	
A16.1.5	Respuesta a incidentes de seguridad de la información	X		
A16.1.6	Aprendizaje de los incidentes de seguridad de la información			X
A16.1.7	Recopilación de evidencias		X	
A17	**Aspectos de seguridad de la información para la gestión de la continuidad de negocio**			
A17.1	**Continuidad de la seguridad de la información**			
A17.1.1	Planificación de la continuidad de la seguridad de la información	X		
A17.1.2	Implementar la continuidad de la seguridad de la información		X	
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información			X
A17.2	**Redundancias**			
A17.2.1	Disponibilidad de los recursos de tratamiento de la información		X	
A18	**Cumplimiento**			
A18.1	**Cumplimiento de los requisitos legales y contractuales**			
A18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	X		
A18.1.2	Derechos de Propiedad Intelectual (DPI)			X
A18.1.3	Protección de los registros de la organización		X	
A18.1.4	Protección y privacidad de la información de carácter personal	X		

A18.1.5	Regulación de los controles criptográficos			X
A18.2	**Revisiones de la seguridad de la información**			
A18.2.1	Revisión independiente de la seguridad de la información			X
A18.2.2	Cumplimiento de las políticas y normas de seguridad			X
A18.2.3	Comprobación del cumplimiento técnico			X
	TOTAL DE CONTROLES	**41**	**44**	**29**

Tabla 5: Controles de anexo A a auditor cada tres años

2.5 GESTIÓN DE INDICADORES

2.5.1 Prologo

En vista que la institución ya tiene planteados los objetivos relacionados a la seguridad de la información es imprescindible realizar un seguimiento para conocer el grado de cumplimiento de los mismos. La gestión de indicadores tiene como propósito establecer métricas que permitan comprobar la efectividad de los mecanismos del Sistema Gestor de Seguridad de la Información en la institución, estos permitirán conocer el estado de los controles y mantenerlos en constante mejoras.

Según la ISO 27001 los indicadores permiten a los directivos tener una perspectiva mucho más clara de que decisiones se deben tomar para optimar los controles de seguridad, puesto que estos presentan suficiente información de manera precisa y medible.

2.5.2 Indicadores

A continuación, tomando como referencia lo dicho por (Rivas, 1988) se procede a definir 10 indicadores que consentirán la administración y el grado de cumplimiento del SGSI, estos se presentan en el gráfico a continuación.

Ilustración 7: Indicadores de cumplimiento del SGSI.

Las tablas a continuación son el detalle de cada indicador. Entre sus campos se encuentra la nomenclatura GIS que hace referencia a Gestión de Indicador de Seguridad, usada para identificar los indicadores acompañada de los números del 01 al 10, también está la abreviatura VGI que significa Variable del Gestor de Indicador acompañada de números para identificar todas las variables usadas en los indicadores. Los indicadores pueden ser de dos tipos: GESTIÓN y CUMPLIMIENTO, para el primero se pueden asignar posibles resultados en porcentajes, es decir que tanto porciento se gestiona el indicador, y para el de cumplimiento se usan dos posibles valores 1 y 0, cumple o no cumple.

<table>
<tr><td>NOMBRE DEL INDICADOR</td><td colspan="5">IMPLEMENTACIÓN DEL SGSI</td></tr>
<tr><td>IDENTIFICADOR</td><td>GIS01</td><td>TIPO</td><td colspan="3">GESTIÓN</td></tr>
<tr><td>OBJETIVO</td><td colspan="5">Verificar la aceptación y uso del SGSI por parte de todo el personal relacionado con la institución.</td></tr>
<tr><td>DEFINICIÓN</td><td colspan="5">Este indicador permite realizar un seguimiento al compromiso de directivos y empleados en lo que refiere a seguridad de la información y docilidad con el SGSI</td></tr>
<tr><td colspan="2">DESCRIPCIIÓN DE VARIABLE</td><td colspan="2">FORMULA</td><td colspan="2">FUENTE DE INFORMACIÓN</td></tr>
<tr><td colspan="2">VGI01: Número total de empleados con roles definidos relacionados con la SI</td><td colspan="2" rowspan="2">$GIS01 = \frac{VGI02\ x\ 100}{VGI01}$</td><td colspan="2">Informe de resultados de auditoria anterior o estado o recomendaciones del SGSI.</td></tr>
<tr><td colspan="2">VGI02: Número de empleados que demuestran procesos relacionados con la SI</td><td colspan="2">Actas de revisión y resultados in situ.</td></tr>
<tr><td colspan="6">METAS</td></tr>
<tr><td>ACEPTABLE</td><td>70%-80%</td><td>DESEABLE</td><td>80% - 90%</td><td>EXCELENTE</td><td>100%</td></tr>
<tr><td>OBSERVACIONES</td><td colspan="5">Según los resultados obtenidos es necesario analizar la matriz de asignación de roles y responsabilidades, no solo para el personal que ya pertenece a la institución, sino también las nuevas contrataciones.</td></tr>
</table>

Tabla 6: Indicador "Implementación del SGSI"

<table>
<tr><td>NOMBRE DEL INDICADOR</td><td colspan="5">DIRECTIVOS INVOLUCRADOS CON LA SI</td></tr>
<tr><td>IDENTIFICADOR</td><td colspan="2">GIS02</td><td>TIPO</td><td colspan="2">GESTIÓN</td></tr>
<tr><td>OBJETIVO</td><td colspan="5">Evaluar que tan dispuestos están los directivos de la institución con la seguridad de la información.</td></tr>
<tr><td>DEFINICIÓN</td><td colspan="5">Conocer el grado de aceptación y adaptación producida de manera general en la institución con procesos relevantes y de dependencia directa con los directivos para poderse cumplir.</td></tr>
<tr><td colspan="3">DESCRIPCIÓN DE VARIABLE</td><td>FORMULA</td><td colspan="2">FUENTE DE INFORMACIÓN</td></tr>
<tr><td colspan="3">VGI03: Matriz de recomendaciones y/o plan de mejora.</td><td rowspan="2">$GIS02 = \frac{VGI04\ x\ 100}{VGI03}$</td><td colspan="2">Informe de resultados de auditoria anterior o estado o recomendaciones del SGSI.</td></tr>
<tr><td colspan="3">VGI04: Cantidad de sugerencias acatadas y solventadas</td><td colspan="2">Actas de revisión y resultados in situ.</td></tr>
<tr><td colspan="6">METAS</td></tr>
<tr><td>ACEPTABLE</td><td>70%-80%</td><td>DESEABLE</td><td>80% - 90%</td><td>EXCELENTE</td><td>100%</td></tr>
<tr><td>OBSERVACIONES</td><td colspan="5">Los directivos deben ser las personas más involucradas en la seguridad de la información y basados en las necesidades detectadas y por prioridad y sensibilidad de los activos, no escatimar recursos para el aseguramiento de los mismos.</td></tr>
</table>

Tabla 7: Indicador "Directivos involucrados con la SI"

<table>
<tr><td>NOMBRE DEL INDICADOR</td><td colspan="3">INCIDENTES DE SEGURIDAD</td></tr>
<tr><td>IDENTIFICADOR</td><td>GIS03</td><td>TIPO</td><td>CUMPLIMIENTO</td></tr>
<tr><td>OBJETIVO</td><td colspan="3">Identificar la efectividad de la gestión de incidentes detectadas el último periodo</td></tr>
<tr><td>DEFINICIÓN</td><td colspan="3">A través de este indicador se podrá conocer que tan efectivos resultaron los procesos de gestión de incidentes mencionados en el SGSI.</td></tr>
<tr><td colspan="2">DESCRIPCIIÓN DE VARIABLE</td><td>FORMULA</td><td>FUENTE DE INFORMACIÓN</td></tr>
<tr><td colspan="2">VGI04: Cantidad de incidentes internos perniciosos detectados.</td><td rowspan="2">Si existiesen incidentes VGI0X = 1

Al no existir incidentes VGI0X = 0</td><td>Informe de resultados de auditoria anterior o estado o recomendaciones del SGSI.</td></tr>
<tr><td colspan="2">VGI05: Cantidad de incidentes externos perniciosos detectados.</td><td>Actas de revisión y resultados in situ.</td></tr>
<tr><td colspan="4">METAS</td></tr>
<tr><td>EXISTEN</td><td>1</td><td>NO EXISTEN</td><td>0</td></tr>
<tr><td>OBSERVACIONES</td><td colspan="3">Si los controles o la gestión de incidentes es la adecuada no deben existir incidentes que perjudiquen los objetivos del negocio.</td></tr>
</table>

Tabla 8: Indicador "Incidentes de Seguridad de la Información"

NOMBRE DEL INDICADOR	USO DE ACTIVOS		
IDENTIFICADOR	GIS04	**TIPO**	CUMPLIMIENTO
OBJETIVO	Verificar el correcto uso y funcionamiento de los activos de información.		
DEFINICIÓN	Indicador que permite conocer si se han aplicado los correctivos en cuanto al mal uso de los activos tecnológicos por parte de los responsables de los mismos.		
DESCRIPCIIÓN DE VARIABLE		**FORMULA**	**FUENTE DE INFORMACIÓN**
VGI06: El activo es usado únicamente por el responsable del mismo.		SE CUMPLE VGI0X = 1 NO SE CUMPLE VGI0X = 0	Inventario de activos.
VGI07: El activo registra uso relacionado con el rol del responsable			Aplicación usada para monitoreo de uso de dispositivos. Logs
VGI08: Se encuentra funcionando el activo o el responsable tiene otro con las mismas funciones			Verificación in situ.
METAS			
SE CUMPLE	**1**	NO SE CUMPLE	0
OBSERVACIONES	Los activos de información deben estar en óptimas condiciones, especialmente en las áreas sensibles.		

Tabla 9: Indicador "Uso de activos"

<table>
<tr><td>NOMBRE DEL INDICADOR</td><td colspan="3">INDUCCIÓN AL PERSONAL</td></tr>
<tr><td>IDENTIFICADOR</td><td>GIS05</td><td>TIPO</td><td>GESTIÓN</td></tr>
<tr><td>OBJETIVO</td><td colspan="3">Comprobar si el personal de la institución conoce las políticas de seguridad de información y el SGSI</td></tr>
<tr><td>DEFINICIÓN</td><td colspan="3">El personal docente, administrativo, de servicios y los clientes de la institución conocen las políticas de seguridad de información y los derechos de privacidad de datos al usar los sistemas de información.</td></tr>
<tr><td colspan="2">DESCRIPCIIÓN DE VARIABLE</td><td>FORMULA</td><td>FUENTE DE INFORMACIÓN</td></tr>
<tr><td colspan="2">VGI09: Cantidad de personas relacionadas con la institución.</td><td rowspan="2">$GIS05 = \frac{VGI10\ x\ 100}{VGI09}$</td><td>Formulario de empleados de la institución. Lista de clientes.</td></tr>
<tr><td colspan="2">VGI10: Cantidad de personas que conocen las políticas de seguridad de la información.</td><td>Encuesta al personal relacionado con la institución.</td></tr>
<tr><td colspan="4">METAS</td></tr>
<tr><td>ACEPTABLE</td><td>80 – 90%</td><td>DESEABLE</td><td>95 -100%</td></tr>
<tr><td>OBSERVACIONES</td><td colspan="3">Todo el personal relacionado con la institución debe formar parte de los procesos de inducción y conocer las políticas de SI asociadas a sus roles y funciones.</td></tr>
</table>

Tabla 10: Indicador "Inducción al personal"

<table>
<tr><td>NOMBRE DEL INDICADOR</td><td colspan="3">SEGURIDAD FÍSICA Y AMBIENTAL</td></tr>
<tr><td>IDENTIFICADOR</td><td>GIS06</td><td>TIPO</td><td>GESTIÓN</td></tr>
<tr><td>OBJETIVO</td><td colspan="3">Identificar si existiesen, vulnerabilidades físicas y ambientales con respecto a la seguridad de los activos de información.</td></tr>
<tr><td>DEFINICIÓN</td><td colspan="3">Se debe garantizar la seguridad física de todos los equipos tecnológicos contemplados en el alcance del SGSI y que en caso de que existiesen inconvenientes naturales estos no afecten el funcionamiento de los mismos.</td></tr>
<tr><td colspan="2">DESCRIPCIIÓN DE VARIABLE</td><td>FORMULA</td><td>FUENTE DE INFORMACIÓN</td></tr>
<tr><td colspan="2">VGI11: Cantidad de equipos/activos de información comprendidos en el alcance del SGSI.</td><td rowspan="2">$GIS05 = \frac{VGI12\ x\ 100}{VGI11}$</td><td>Inventario de activos en el SGSI.</td></tr>
<tr><td colspan="2">VGI12: Cantidad de equipos/activos en los cuales se comprueba es seguro el acceso físico no autorizado e inmune a problemas ambientales.</td><td>Verificación in situ.</td></tr>
<tr><td colspan="4">METAS</td></tr>
<tr><td>ACEPTABLE</td><td>80 – 90%</td><td>DESEABLE</td><td>95 -100%</td></tr>
<tr><td>OBSERVACIONES</td><td colspan="3">Se debe procurar que todos los activos de información se encuentran en lugares con temperaturas adecuadas y seguros frente a hurtos, problemas ambientales, incendios, inundaciones, etc.</td></tr>
</table>

Tabla 11: Indicador "Seguridad física y ambiental"

NOMBRE DEL INDICADOR	CONTROL DE ACCESO		
IDENTIFICADOR	GIS07	**TIPO**	CUMPLIMIENTO
OBJETIVO	Identificar la aplicación controles existentes relacionados con estándares o normas para controlar la accesibilidad de los activos.		
DEFINICIÓN	Niveles de control de accesos aplicados en la institución.		
DESCRIPCIIÓN DE VARIABLE		**FORMULA**	**FUENTE DE INFORMACIÓN**
VGI13: Se han establecido normas de acceso para que los usuarios accedan y usen sus equipos informáticos.		SE EVIDENCIA VGI0X = 1	Usuarios internos.
VGI14: Se han establecido normas de acceso para los sistemas de información.		NO SE EVIDENCIA VGI0X = 0	Usuarios internos.
METAS			
CUMPLE	1	**NO CUMPLE**	0
OBSERVACIONES	Deben haber normas claras y precisas referentes al acceso a activos de información.		

Tabla 12: Indicador "Control de acceso"

<table>
<tr><td>NOMBRE DEL INDICADOR</td><td colspan="3">BACKUPS</td></tr>
<tr><td>IDENTIFICADOR</td><td>GIS08</td><td>TIPO</td><td>CUMPLIMIENTO</td></tr>
<tr><td>OBJETIVO</td><td colspan="3">Identificar los procesos de respaldo de información en los sistemas informáticos.</td></tr>
<tr><td>DEFINICIÓN</td><td colspan="3">Guardar la información almacenada por cierto tiempo el sistemas informáticos en otro dispositivo fuera de línea o inaccesible personas no autorizadas.</td></tr>
<tr><td colspan="2">DESCRIPCIIÓN DE VARIABLE</td><td>FORMULA</td><td>FUENTE DE INFORMACIÓN</td></tr>
<tr><td colspan="2">VGI15: Se realiza backup completos en los activos de información.</td><td rowspan="3">SE EVIDENCIA VGI0X = 1

NO SE EVIDENCIA VGI0X = 0</td><td>Registro de backups.</td></tr>
<tr><td colspan="2">VGI16: Se realiza backup incrementales en los activos de información.</td><td>Registro de backups.</td></tr>
<tr><td colspan="2">VGI17: Se realiza backup diferenciales en los activos de información.</td><td>Registro de backups.</td></tr>
<tr><td colspan="4">METAS</td></tr>
<tr><td>CUMPLE</td><td>1</td><td>NO CUMPLE</td><td>0</td></tr>
<tr><td>OBSERVACIONES</td><td colspan="3">El respaldo de la información es un proceso esencial para el aseguramiento de la información.</td></tr>
</table>

Tabla 13: Indicador "Backups"

<table>
<tr><td>NOMBRE DEL INDICADOR</td><td colspan="3">PROTECCIÓN CONTRA SOFTWARE MALICIOSO</td></tr>
<tr><td>IDENTIFICADOR</td><td>GIS09</td><td>TIPO</td><td>CUMPLIMIENTO</td></tr>
<tr><td>OBJETIVO</td><td colspan="3">Conocer la eficiencia de los controles aplicados para evitar la infección de software malicioso.</td></tr>
<tr><td>DEFINICIÓN</td><td colspan="3">Normas, configuraciones y software usado para evitar la infección de virus, gusanos o cualquier otro software malicioso.</td></tr>
<tr><td colspan="2">DESCRIPCIIÓN DE VARIABLE</td><td>FORMULA</td><td>FUENTE DE INFORMACIÓN</td></tr>
<tr><td colspan="2">VGI17: Se ha instalado y actualizado antivirus en los equipos/activos de información.</td><td rowspan="2">SE EVIDENCIA VGI0X = 1

NO SE EVIDENCIA VGI0X = 0</td><td>Logs de antivirus y de aplicaciones de monitoreo.</td></tr>
<tr><td colspan="2">VGI18: Se monitorea constantemente los registros para verificar la ejecución de programas desconocidos.</td><td>Logs de antivirus y de aplicaciones de monitoreo.</td></tr>
<tr><td colspan="4">METAS</td></tr>
<tr><td>CUMPLE</td><td>1</td><td>NO CUMPLE</td><td>0</td></tr>
<tr><td>OBSERVACIONES</td><td colspan="3">Los antivirus deben estar en la capacidad de detectar cualquier anomalía en los procesos de sistemas y aplicaciones de los activos de información.</td></tr>
</table>

Tabla 14: Indicador "Protección contra software malicioso"

<table>
<tr><td>NOMBRE DEL INDICADOR</td><td colspan="5">ANÁLISIS DE VULNERABILIDADES</td></tr>
<tr><td>IDENTIFICADOR</td><td colspan="2">GIS10</td><td>TIPO</td><td colspan="2">GESTIÓN</td></tr>
<tr><td>OBJETIVO</td><td colspan="5">Disminuir la cantidad de vulnerabilidades que de ser explotadas perjudiquen el funcionamiento de los sistemas de información.</td></tr>
<tr><td>DEFINICIÓN</td><td colspan="5">Las vulnerabilidades o brechas de seguridad existentes deben ser disminuidas al máximo.</td></tr>
<tr><td colspan="3">DESCRIPCIIÓN DE VARIABLE</td><td>FORMULA</td><td colspan="2">FUENTE DE INFORMACIÓN</td></tr>
<tr><td colspan="3">VGI21: Cantidad de vulnerabilidades detectadas en el SGSI.</td><td rowspan="2">$GIS10 = \frac{VGI22\ x\ 100}{VGI21}$</td><td colspan="2">Fase de análisis de riesgos del SGSI.</td></tr>
<tr><td colspan="3">VGI22: Cantidad de vulnerabilidades encontradas en la nueva revisión.</td><td colspan="2">Resultado de análisis de riesgos actual</td></tr>
<tr><td colspan="6">METAS</td></tr>
<tr><td>MÁXIMO</td><td>30% - 20%</td><td>DESEABLE</td><td>20% - 10%</td><td>EXCELENTE</td><td>5% - 0%</td></tr>
<tr><td>OBSERVACIONES</td><td colspan="5">El porcentaje de vulnerabilidades detectadas con referencia al control anterior debe disminuir periódicamente.</td></tr>
</table>

Tabla 15: Indicador "Análisis de vulnerabilidad"

2.6 PROCEDIMIENTO DE REVISION POR DIRECCIÓN

2.6.1 Prologo

Con el propósito de evaluar la efectividad, eficiencia, buen funcionamiento del Sistema Gestor de Seguridad de la Información y determinar si los recursos asignados para realzar este proceso valen la pena, es imprescindible que la alta dirección o directivos que son la máxima autoridad de la institución y los mayores responsables del SGSI realicen revisiones periódicas al sistema planteado, este proceso permitirá eliminar no conformidades detectadas y establecer un plan de mejora frente a este tipo de

situaciones. La ISO 27001 propone una serie de indicaciones para realizar el procedimiento de revisión por parte de los directivos institucionales.

2.6.2 Procedimiento

La labor de revisión es un proceso que se debería hacer con una periodicidad de un año o menos dependiendo la criticidad con la que se encontraba la institución previa a la SGSI, a continuación, se muestra el proceso.

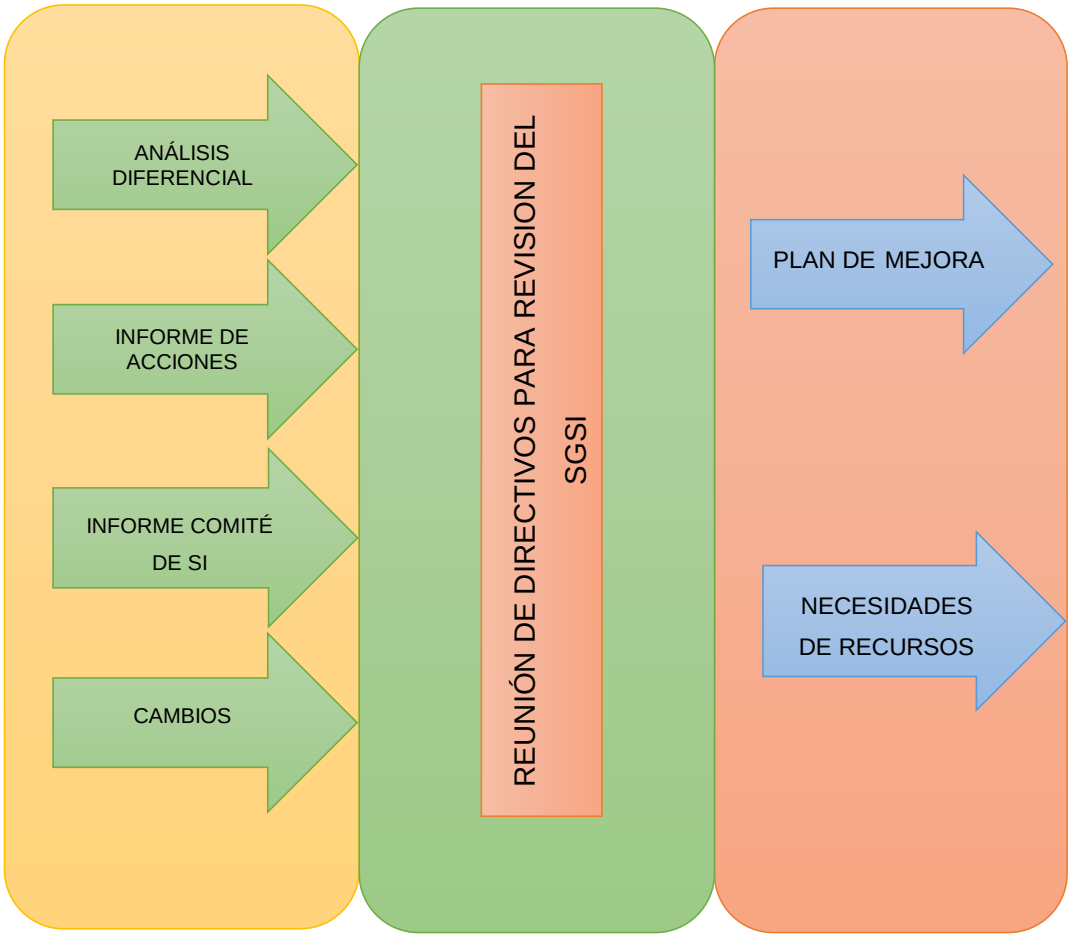

Ilustración 8: Proceso de auditoría de Seguridad de Información.

2.6.3 ENTRADAS

Análisis diferencial: Es importante presentar de una manera resumida, con lenguaje sencillo entendible para todos los presentes, el responsable de seguridad debe presentarlo al resto de directivos y realizar las aclaraciones necesarias. Esta entrada permitirá conocer la situación actual de la institución referente a los controles y procesos asociados a la seguridad de la información, los resultados se muestran en porcentajes, lo cual hará posible una clara percepción de los resultados.

Informe de acciones: Los directivos deben poder analizar las acciones realizadas en relación al resultado de las reuniones anteriores y aprobación del SGSI, estas deben

estar acompañadas de los recursos provistos y el tiempo tomado para la ejecución de las mismas.

Informe del comité de Seguridad de la Información: Este comité representado por el responsable de Seguridad de la Información debe presentar el informe de las apreciaciones, observaciones, recomendaciones y cualquier otro documento que permita a los directivos conocer a detalle cómo se encuentra la situación frente a un nuevo Sistema Gestor de Seguridad de la Información o el avance perpetrado en el último periodo del ya existente. Aquí se debe adjuntar los indicadores resultantes del proceso anterior

Cambios: Hace referencia a todos los cambios realizados en la institución que pueden estar relacionado con los activos y sistemas de información comprendidos en el alcance del SGSI, estos pueden ser adquisiciones de nuevos equipos o sistemas de información, nuevos negocios con entes externas relacionada con la TI, modificaciones en responsabilidades y/o roles asociadas a la SI, etc. No debe pasar desapercibido ningún elemento con el tema en relación.

Los puntos de revisión por la dirección según la ISO 27001 son:

- ✓ Resultados de la auditoría (si existiese)
- ✓ El estado de las acciones de revisiones de gestión anteriores;
- ✓ Cambios en problemas externos e internos que son relevantes para el sistema de gestión de la seguridad de la información;
- ✓ Retroalimentación sobre el desempeño de la seguridad de la información.
- ✓ No conformidades y acciones correctivas.
- ✓ Resultados de monitoreo y medición.
- ✓ Cumplimiento de los objetivos de seguridad de la información.
- ✓ Retroalimentación de las partes interesadas;
- ✓ Los resultados de la evaluación de riesgos y el estado del plan de tratamiento de riesgos;
- ✓ Las oportunidades para la mejora continua.
- ✓ Planificar las fechas y el esquema de la próxima auditoría.

2.6.4 PROCESO

Reunión de los directivos: La alta dirigencia de la institución formada por los coordinadores departamentales, representante legal y funcionarios con roles directivos deben sesionar en reunión con el fin de analizar las entradas destinadas para este proceso, es importante todos se involucren y realicen aportes para evaluar la implementación del Sistema de Gestión de Seguridad de la Información y de ser

necesario sumar experiencias y contribuciones generales que permiten fortificar el SGSI. Aquí se deben tomar decisiones transcendentales de aporte para el SGSI. La convocatoria puede hacerse de manera electrónica a través de correo o de manera física con registro de firmas de los convocados.

2.6.5 SALIDAS

Plan de mejora: Estas son una serie de acciones a realizarse para mejorar los inconvenientes detectados en la reunión de directivos, es importante que se establezcan fechas y responsables de cada actividad, es importante evitar inmiscuir al responsable de seguridad en las actividades puesto que esta persona estará al frente de todo el plan de mejora y de manera interna evaluará el cumplimiento de las mismas. Se debe contemplar cada una de las etapas del SGSI y si es necesario realizar una nueva versión del mismo, es preciso abordar la gestión de riesgos y vulnerabilidades, continuidad de negocio y abordaje de activos de información contemplados en el plan de seguridad.

Necesidades de recursos: Contemplado el plan de mejora y los resultados de la reunión de directivos deben destinarse los recursos necesarios para garantizar se cumplan los objetivos de la seguridad de información y el SGSI, estos recursos deben ser asignados con fechas progresivas de acuerdo a la prioridad a la que fueron destinados los mismos, de ser recursos económicos los que se ven involucrados debe existir un presupuesto asignado al proyecto, este descrito y adaptado frente a cualquier índole por la persona responsable de finanzas, miembro también de los directivos.

Al final de la reunión se deben tomar las siguientes decisiones:

- ✓ Si el SGSI ha cumplido sus objetivos
- ✓ Qué mejoras son necesarias
- ✓ Si es necesario realizar cambios en el alcance
- ✓ Aprobar los recursos necesarios para los controles y procesos de la Seguridad de la información
- ✓ Si es necesario realizar modificaciones en los documentos principales.

Al finalizar la reunión debe emitirse un acta con todos los puntos tratadas, ésta en un lapso de tiempo no mayor a 24 horas debe ser enviada por correo a todos los participantes para su revisión y observaciones, para posteriormente proceder a la firmas y ejecución de los procesos mencionados.

2.7 GESTIÓN DE ROLES Y RESPONSABILIDADES

2.7.1 Prólogo

Al momento de la implementación del Sistema Gestor de Seguridad de la Información es de carácter obligatorio establecer una estructura organizacional con roles, funciones y responsabilidades enmarcadas en torno al SGSI, con el propósito de ejecutar las actividades que este requiere para su implementación, este proceso es tan necesario al punto que es posible que no se cumplan en su totalidad las acciones que no tengan asignado un responsable.

Cuando la persona asume un rol, debe trazarse como metas cumplir de manera eficiente y eficaz los objetivos contemplados en las tareas de las funciones asignadas e informar a la alta dirección a través de documentos electrónicos los avances logrados de manera progresiva.

Las responsabilidades asignadas a cada rol dependen de los objetivos planteados a las diferentes actividades, estas permitirán conocer el alcance mínimo y máximo que deben tener los responsables en la implementación del SGSI

2.7.2 Objetivos

Asignar e identificar los roles con sus respectivas funciones y responsabilidades al personal involucrado con el plan de seguridad de la información.

2.7.3 Asignaciones y perfiles

MATRIZ DE ASIGNACION DE ROLES ASOCIADAS AL SGSI EN LA UESMA			
ID	NOMBRE DEL ROL	RESPONSABLES	FUNCIONES

RSI01	DIRECTIVOS	-Director General -Coordinador General -Rector -Coordinador de TIC -Coordinador de Finanzas -Coordinador de gestión de talento humano -Coordinador DECE -Coordinador de DPEI	Hacer que la seguridad de la información sea un punto en la agenda de reuniones del comité. Designar roles y funciones a los miembros del SGSI y asignar recursos. Aprobar el plan de seguridad de la información y cualquier otro documento resultante. Evaluar los informes proveídos por los demás roles y departamentos. Determinar el umbral de riesgo aceptable relacionado a la SI. Realizar los cambios necesarios en el personal asignado para la SI. Realizar seguimiento de ejecución de tareas. Aprobar adquisición de recursos necesarios para la SI. Calendarizar el plan de mejora y hacer seguimiento. Convocar reuniones de directivos o comité de seguridad.
RSI02	Responsable de seguridad de la información	Coordinador del departamento de TICs	Proponer las políticas de seguridad de la información. Liderar las auditorías internas de SI. Gestionar de manera general la Seguridad de la Información.

			Administrar la gestión de riesgos e incidentes en conjunto con las áreas del negocio. Establecer directrices para el comité de seguridad de la información. Gestionar el plan de inducción de SI y realizar seguimiento de cumplimiento de las mismas. Definir la arquitectura de seguridad de los sistemas de información. Establecer las funciones dentro del SGSI.
RSI03	Comité de seguridad	-Coordinador de TICs -Coordinadores de cada departamento de la institución. ***Ver organigrama en la fase 1 del SGSI.***	Coordinar la implementación en cada departamento del SGSI. Impulsar los proyectos del área de seguridad de la información Revisar el estado de avance del proyecto de SI. Proponer funciones, responsabilidades y roles enmarcados en la SI. Realizar las auditorías internas. Proponer los recursos necesarios para salvaguardar la seguridad de la información. Proponer y promover la difusión de las políticas de seguridad de la información.
RSI04	Responsable de seguridad física y ambiental.	Coordinador general	Gestionar las adecuaciones necesarias para garantizar la seguridad física y ambiental de los activos de información.

			Disponer las medidas de recuperación y aseguramiento de activos frente a catástrofes ambientales. Reportar los incidentes o brechas de seguridad detectadas asociadas a los activos de información. Proponer a los directivos la asignación de recursos para la ejecución de tareas asociadas a la función.
RSI05	Asesor Jurídico	Coordinador del departamento jurídico.	Trabajar en conjunto con el comité de seguridad para verificar la legalidad de las políticas de seguridad de la información. Garantizar la privacidad y derechos que debe tener el personal asociado a la institución en torno a la seguridad de la información. Detectar todas leyes, normas, reglamentos y cualquier otro documento de carácter legal asociado a la seguridad de la información. Verificar el cumplimiento de las políticas de seguridad de la información en el cese de funciones de los ex empleados de la institución. Elaborar documentos de acuerdos y responsabilidades y constatar firmas de conocimiento

			y aceptación de políticas de seguridad de la información.

Tabla 16: Roles y responsabilidades entorno al SGSI

2.8 METODOLOGÍA DE ANALISIS DE RIESGOS

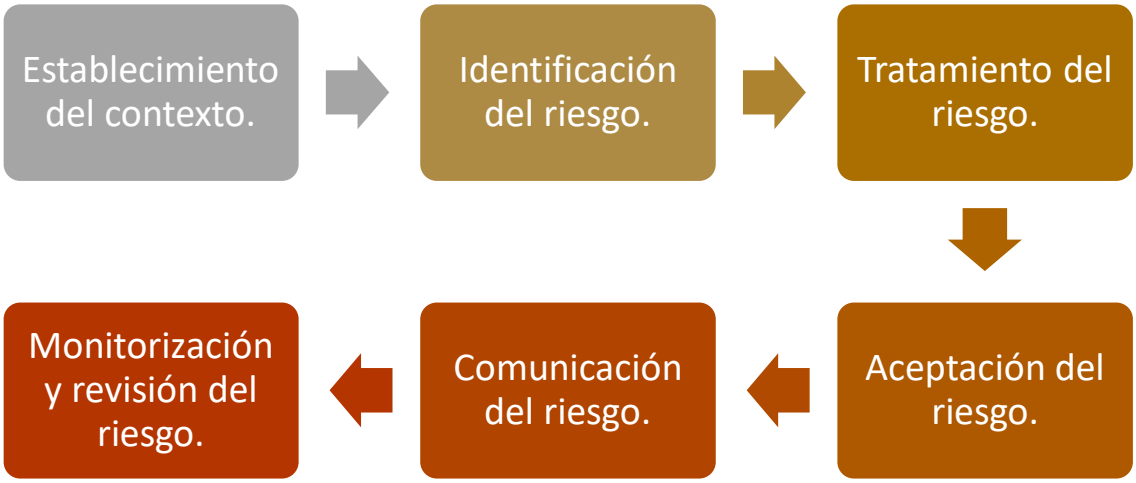

Ilustración 9: Proceso de análisis de riesgos.

2.8.1 Establecimiento Del Contexto

La realización del contexto permitirá a la institución modular los objetivos relacionados con la seguridad de la información, definir y clasificar los parámetros internos y externos y definir de manera correcta los criterios de riesgos relacionados al proceso general de la gestión de los mismos.

Debe ser analizada y establecida toda información relacionada al contenido de la gestión de riesgos asociados a los activos de información de la institución, es decir, la totalidad de las circunstancias que hacen posible, condicionan o determinan la realización de este proceso, estos contextos pueden ser externos o internos, para recaudar esta información de índole primordial se puede partir de conocer la institución, entrevistas con directivos, jefes departamentales, empleados en general y clientes.

Al finalizar se establece el alcance de la gestión de riesgos y las responsabilidades dentro de este proceso y como resultado deben ser determinados los siguientes propósitos:

Alcance, límites y restricciones de la Gestión de Riesgos de Seguridad de la Información.

- ✓ Criterios para la evaluación de riesgos.
- ✓ Criterios de impacto.
- ✓ Criterios para la aceptación de riesgos.
- ✓ Organización para la gestión de riesgos.

2.8.2 Identificación Del Riesgo.

Concluida la contextualización del análisis de riesgos y la definición del alcance y restricciones comprendidas, en la identificación del riesgo se pretende analizar y evaluar los mismos, como se expresa en el siguiente gráfico.

Identificación del riesgo	Análisis del riesgo	Evaluación del riesgo
• Se determinan los eventos que pueden causar perdidas potenciales relacionadas a los activos de información.	• Se establece y se identifican las probabilidades de que ocurran estos eventos.	• Asocia los riesgos de acuerdo a los criterios de evaluación establecidos en la definición del contexto.

Ilustración 10: Proceso de identificación de riesgos

Es de carácter obligatorio e indispensable que la institución identifique las fuentes de riesgos, que las causa y las consecuencias en caso de consumarse, este proceso tiene como propósito detallar una lista con el registro de eventos que alteran el funcionamiento normal de los sistemas de información de la institución y retrasa o impide la consecución de objetivos institucionales, es decir, deben estar identificados los eventos que pudiesen causar pérdidas en el negocio.

Para esto, como primera parte se deben identificar y clasificar los activos tecnológicos, el responsable de este debe estar definido en esta etapa.

Activos primarios

Son las actividades y procesos relacionados directamente con los objetivos del negocio y la información relacionada a estos, una manera muy acertada de identificar estos activos es a traves de entrevistas dirigidas a todos los jefes departamentales y el director general de la institución. Estos activos pueden ser:

*Procesos, subprocesos y actividades de negocio en las cuales de verse interrumpidas impide a la institución continuar con los procesos del negocio.

*Información indispensable para la consecución de las actividades fundamentales de la organización y aquella considerada de carácter personal de empleados o clientes.

Activos de infraestructura y soporte

Para la identificación de este tipo de activos es sustancial incluir nuevas entrevistas de ser necesario y observaciones in situ para tener la información suficiente para determinar cuáles son los activos de infraestructura.

Los activos comprendidos en esta sección tienen la característica de ser objetos o personas sirven de medio para la efectuación de los activos primarios, si se presenta inconvenientes en su funcionamiento pueden ser reemplazados sin afectar directamente los procesos del negocio, estos pueden ser equipos informáticos como hardware y software, infraestructura de red y el personal

Identificación de amenazas

Teniendo claro el concepto de amenazas, para la identificación de las mismas es necesario conocer el historial de incidentes ocurridos, observaciones realizadas por los responsables de los sistemas información y relacionar con las amenazas externas conocidas, con esto se podrá clasificar las amenazas y determinar su origen.

Identificación de la fuente de la amenaza y su agente

Las amenazas pueden comprometer gravemente los activos y por lo tanto es esencial identificarlas

Se entiende por agente de una amenaza a la entidad con capacidad de fundar una amenaza capaz de explotar y descubrir alguna vulnerabilidad.

Las amenazas pueden ser de origen natural, ambiental, accidentales o premeditadas.

Para la correcta identificación de las amenazas se puede usar verificación in situ, entrevistas y análisis de herramientas usadas en este tipo de procesos.

Es muy posible que se vean perjudicados más de un activo por una sola amenaza, cuando esto sucede el equipo gestor de análisis deben considerar que una misma amenaza puede afectar de distintas maneras a varios activos.

La información obtenida en este proceso debe ser considerada de carácter sensible-confidencial, y como tal debe ser correctamente custodiada y tratada.

Identificar controles existentes

Los controles pueden ser estructuras definidas de la institución, políticas de seguridad, procesos, configuraciones, parches, antivirus, cerraduras, extintor, baterías de almacenamiento de energía eléctrica y un sin número más de actividades que pueden servir de controles.

En este proceso de identificación pueden ser tomados los controles evidencialmente planificados para implementarse y los que ya se encuentran en ejecución, por lo tanto, deben tomarse estos datos de los planes de tratamiento de riesgos y la documentación que respaldo este proceso, el procesamiento de estos dará como resultado una lista de controles planificados y en ejecución acompañados del estado de uso en el que se encontrasen. Realizar de manera correcta la identificación de los controles evitará controles duplicados lo que conlleva a despilfarro de recursos, para ello se deben realizar reuniones con el comité de seguridad de la información, entrevistas con usuarios internos y externos para detectar los controles y la efectividad de los mismos, análisis exhaustivo de la documentación que respalda los controles existentes, check lists y cuestionarios y verificaciones in situ.

Es necesario hacer énfasis en que posiblemente un control puede fallar y dependiendo la sensibilidad del activo de información puede existir un control alternativo que entra en ejecución cuando el principal no cumple su objetivo, lo ideal es implementar el mejor control en estos casos.

Análisis de riesgos

Esta actividad permite identificar la relación entre las amenazas y las vulnerabilidades y así categorizar el riesgo ocasionado y asignarle el tratamiento idóneo para el mismo, las amenazas en este punto ya se conocen, lo siguiente es definir las vulnerabilidades, proceso detallado a continuación:

Identificación de vulnerabilidades

En la ejecución este proceso sistemático se deben analizar los siguientes puntos

- ✓ Procesos y procedimientos.

- ✓ Estructura organizacional.
- ✓ Contratos internos y externos.
- ✓ Instalaciones físicas y alrededores.
- ✓ Frecuencia de eventos de desastres naturales.
- ✓ Configuración y características de los sistemas de información.
- ✓ Infraestructura de red y comunicación.
- ✓ Hardware y software.

Para ello pueden usarse herramientas código abierto y privativas que permiten detectar vulnerabilidades, pruebas de seguridad en diferentes escenarios físicos y lógicos, test de penetración. Como resultado se conocerán las vulnerabilidades asociadas a los activos de información y las amenazas arraigadas a estos que fueron identificadas previamente, puesto que el simple hecho de la existencia de una vulnerabilidad no significa que el activo está en riesgo

Identificación de consecuencias.

Esta actividad forma parte del análisis de riesgos y su principal objetivo es identificar los escenarios en los cuales una amenaza asecha una vulnerabilidad y determinar las situaciones de efectuarse, entre estas se encuentran:

- Perdida de información.
- Afectaciones en el personal de la institución.
- Inversión de recursos para investigar y reparar el inconveniente
- Perdida de reputación del negocio.
- Inestabilidad en el funcionamiento de los activos.
- Violación de derechos y obligaciones contempladas en políticas internas y demás documentos legales
- Perdidas económicas

Evaluación del riesgo

Posterior a la etapa de análisis de riesgos es necesario se asigne valores a los activos para así determinar la prioridad con la que debe ser tratados los riesgos, en vista que la institución tendrá claro la representatividad cualitativa y/o cuantitativa que tiene los activos de información, para ello es necesario los resultados de las etapas y procesos anteriores realizados de acuerdo a la seguridad de la información y los detalles de funciones y costos de la implementación de los sistemas de información.

Análisis cualitativo.

Este análisis se basa en la evaluación de cualidades, usando atributos, descripciones, determinadores, calificadores que permitan apreciar en un lenguaje básico (no usado en operaciones matemáticas) las consecuencias y la posibilidad de ocurrencia de riesgos identificados, son usadas escalas de adjetivos que no determinan un valor financiero de los procesos y activos detallados. Estos atributos pueden ser:

Para consecuencias

- Irrelevante, Insignificante, Marginal, Critico, Extremo, Catastrófico.
- Extremo, alto, medio, bajo, imperceptible.
- Grande, mediana, pequeña, muy pequeña.

Para probabilidades:

- Alta, Media, Baja
- Escaso, Poco posible, posible, Muy posible.
- Nunca, Casi nunca, Ocasionalmente, Varias veces, Seguido, Muy a menudo

Análisis cuantitativo

A diferencia del anteriormente descrito, este usa valores numéricos que pueden ser usados en operaciones matemáticas que permitan conocer un total o determinaciones a través de fórmulas matemáticas, estos son generalmente valores financieros, aunque estos no sean totalmente precisos también para el uso de niveles porcentuales y estadísticos, pueden ser:

Consecuencias

- Costo de reposición del activo.
- Costo de mantenimiento del activo.
- Costo de la multa o compensación al incumplir alguna política, norma o ley.
- Costo de las pérdidas generadas.

2.8.3 Tratamiento del riesgo.

Hasta este punto los responsables de seguir el SGSI cumplen la función de recaudación de información, real y de contraste para poder conocer la realidad de los activos de información con respecto a la seguridad y priorizar los riesgos en la forma que deben ser tratados, por lo tanto, es preciso que el equipo evalué los procesos realizados hasta este momento y compruebe que es el más idóneo, de no ser así se sugiere volver a empezar con la etapa de contextualización. De considerarse adecuado se procede a

analizar los resultados, que en resumen serían los riesgos ordenados de acuerdo a su prioridad acompañado de los escenarios de incidentes, como resultado se establecerá que hacer con los riesgos y conocer los riesgos residuales, por lo tanto, el comité de seguridad debe elaborar un plan de tratamiento de riesgos que busca reducir la afectación de los mismos; existen 4 opciones para tratar el riesgo: modificar, retener, evitar y compartir el riesgo, estas serán determinadas dependiendo el análisis realizado por el equipo de seguridad y las capacidades de la institución.

Modificar el riesgo

- Aplicar controles que reduzcan los riesgos a niveles aceptables.
- Se deben considerar los criterios de la institución para aceptar el riesgo.
- Como resultado posteriormente puede darse un tratamiento de riesgos diferente.

Retener el riesgo.

- Es la aceptación de que ocurriese un riesgo.
- Se deben considerar los riesgos no identificados.
- Se deben realizar de acuerdo a los criterios de aceptación de riesgo ya definidos.
- Registrar los riesgos asumidos y realizar seguimiento.

Evitar el riesgo.

- Se aplica a riesgos considerados extremadamente altos.
- Si el control consume más recursos que los beneficios obtenidos por el activo.
- Puede ser necesario eliminar la actividad o proceso.

Compartir el riesgo.

- Involucra a una entidad externa que se encarga del riesgo.
- Uso de seguros que cubran consecuencias de incidentes de seguridad de información.
- Las consecuencias legales asociadas a un riesgo no pueden ser transferidas.

Riesgos residuales.

Los riesgos residuales consisten en determinar los riesgos que persisten habiendo aplicado ya el tratamiento de riesgos, es decir posterior a los controles es posible que no se suficiente para que el riesgo no resulte perjudicial para los objetivos del negocio. Si este riesgo está por encima del umbral de riesgo determinado en fases anteriores debe aplicarse los controles necesarios para realizar un correcto tratamiento. Son considerados también riesgos residuales aquellos de poca importancia o los que deben ser aceptados.

2.8.4 Comunicación del riesgo

Esta actividad se realiza en paralelo a las fases anteriores relacionadas a los riesgos, esto mantendrá informados a los directivos y responsables de los activos de información sobre el estado de los mismos y el proceso del SGSI, es una tarea esencial para procurar que todos se involucren en la Seguridad de la Información y facilite la toma de decisiones que se consideren necesarias. La documentación se debe realizar de manera formal a través de documentos, reuniones periódicos o percepción del trabajo realizado en tiempo real.

2.8.5 Monitorización y revisión del riesgo

También debe considerarse esta actividad en todas las fases del análisis de riesgo, permite la verificación control de resultados, este es un proceso sistemático que permite recopilar información de la gestión de riesgos, se obtiene a través del acompañamiento de todas las actividades realizando un análisis crítico en cada fase. La comunicación y la monitorización están ligadas y ambas deben ser realizadas simultáneamente al resto de las actividades de gestión de riesgos y permitirán detectar inconsistencias en las mismas.

2.9 DECLARACIÓN DE APLICABILIDAD

Concluida la fase de análisis de riesgo se tienen claros los controles provenientes de la norma IEC/ISO 27001 que deben ser aplicados por la institución, los directivos deben aprobar la implementación de los nuevos controles y los que ya tiene la organización, a este documento se le denomina **declaración de aplicabilidad**.

Sección	Controles de Seguridad de la Información	APLICA	JUSTIFICACIÓN
A5	**Políticas de seguridad de la información**		
A5.1	**Directrices de gestión de la seguridad de la información**		
A5.1.1	Políticas para la seguridad de la información	SI	
A5.1.2	Revisión de las políticas para la seguridad de la información	SI	Esencial en el SGSI
A6	**Organización de la seguridad de la información**		
A6.1	**Organización interna**		

A6.1.1	Roles y responsabilidades en seguridad de la información	SI	Es necesario identificar responsables de cada tarea
A6.1.2	Segregación de tareas	SI	
A6.1.3	Contacto con las autoridades	SI	Las autoridades deben estar involucradas con el SGSI
A6.1.4	Contacto con grupos de interés especial	SI	El comité de la seguridad debe precautelar la seguridad en todos los proyectos tercerizar los procesos necesarios
A6.1.5	Seguridad de la información en la gestión de proyectos	SI	
A6.2	**Los dispositivos móviles y el teletrabajo**		
A6.2.1	Política de dispositivos móviles	SI	BYOD es aplicado y debe definirse las restricciones de uso
A6.2.2	Teletrabajo	NO	No se realiza trabajo desde afuera sobre los sistemas de información
A7	**Seguridad relativa a los recursos humanos**		
A7.1	**Antes del empleo**		
A7.1.1	Investigación de antecedentes	SI	Es necesario conocer las referencias del empleado y comunicar las normativas de la institución para así el trabajador conozca sus deberes, derechos y responsabilidades incluso en el cese de funciones.
A7.1.2	Términos y condiciones del empleo	SI	
A7.2	**Durante el empleo**		
A7.2.1	Responsabilidades de gestión	SI	
A7.2.2	Concienciación, educación y capacitación en seguridad de la información	SI	
A7.2.3	Proceso disciplinario	SI	
A7.3	**Finalización del empleo o cambio en el puesto de trabajo**		
A7.3.1	Responsabilidades ante la finalización o cambio	SI	

A8	**Gestión de activos**		
A8.1	**Responsabilidad sobre los activos**		
A8.1.1	Inventario de activos	SI	Deben estar cuantificados los activos de información y asociados a un responsable que debe procurar se le de uso relacionado a sus actividades, se debe además realizar control de permanencia y devolución al finalizar la función asociada.
A8.1.2	Propiedad de los activos	SI	
A8.1.3	Uso aceptable de los activos	SI	
A8.1.4	Devolución de activos	SI	
A8.2	**Clasificación de la información**		
A8.2.1	Clasificación de la información	SI	La información debe estar correctamente clasificada y definir la administración sobre la misma, es el activo más importante.
A8.2.2	Etiquetado de la información	SI	
A8.2.3	Manipulado de la información	SI	
A8.3	**Manipulación de los soportes**		
A8.3.1	Gestión de soportes extraíbles	SI	Los medios extraíbles por su función son propensos a introducir amenazas para la institución por lo tanto debe estar clara la política del uso y de recisión
A8.3.2	Eliminación de soportes	SI	
A8.3.3	Soportes físicos en tránsito	SI	
A9	**Control de acceso**		
A9.1	**Requisitos de negocio para el control de acceso**		
A9.1.1	Política de control de acceso	SI	

A9.1.2	Acceso a las redes y a los servicios de red	SI	Se debe definir el uso de los sistemas de información y la infraestructura TI para evitar desperdicios de recursos.
A9.2	**Gestión de acceso de usuario**		
A9.2.1	Registro y baja de usuario	SI	Cada activo de información debe tener definido sus usuarios y los alcances de los mismos sobre este, al finalizar un empleado sus funciones deben ser retirados los privilegios sobre los SI
A9.2.2	Provisión de acceso de usuario	SI	
A9.2.3	Gestión de privilegios de acceso	SI	
A9.2.4	Gestión de la información secreta de autenticación de los usuarios	SI	
A9.2.5	Revisión de los derechos de acceso de usuario	SI	
A9.2.6	Retirada o reasignación de los derechos de acceso	SI	
A9.3	**Responsabilidades del usuario**		
A9.3.1	Uso de la información secreta de autenticación	SI	Posterior al etiquetado de información y responsabilidad se podrá definir políticas de confidencialidad sobre la información que corresponda.
A9.4	**Control de acceso a sistemas y aplicaciones**		
A9.4.1	Restricción del acceso a la información	SI	La implementación de un sistema centralizado de control de usuarios es necesario para poder garantizar y controlar la accesibilidad de la información.
A9.4.2	Procedimientos seguros de inicio de sesión	SI	
A9.4.3	Sistema de gestión de contraseñas	SI	
A9.4.4	Uso de utilidades con privilegios del sistema	SI	
A9.4.5	Control de acceso al código fuente de los programas	SI	
A10	**Criptografía**		
A10.1	**Controles criptográficos**		

A10.1.1	Política de uso de los controles criptográficos	SI	Existen procesos en los cuales se usa firma electrónica y token de aprobación, por lo tanto deben ser definidas la políticas de custodia y uso sobre estos.
A10.1.2	Gestión de claves	SI	
A11	**Seguridad física y del entorno**		
A11.1	**Áreas seguras**		
A11.1.1	Perímetro de seguridad física	SI	La infraestructura física es un factor importante para precautelar la seguridad de los activos y el recurso humano
A11.1.2	Controles físicos de entrada	SI	
A11.1.3	Seguridad de oficinas, despachos y recursos	SI	
A11.1.4	Protección contra las amenazas externas y ambientales	SI	
A11.1.5	El trabajo en áreas seguras	SI	
A11.1.6	Áreas de carga y descarga	SI	
A11.2	**Seguridad de los equipos**		
A11.2.1	Emplazamiento y protección de equipos	SI	Los equipos y la infraestructura de comunicación debe estar funcional siempre, por lo tanto es importante que se establezcan medidas de seguridad para garantizar la continuidad de los mismos frente a diferentes incidentes
A11.2.2	Instalaciones de suministro	SI	
A11.2.3	Seguridad del cableado	SI	
A11.2.4	Mantenimiento de los equipos	SI	
A11.2.5	Retirada de materiales propiedad de la empresa	SI	Se debe garantizar la seguridad sobre los equipos que son usados fuera de la institución y existir políticas en caso de cualquier inconveniente sobre estos incluso al ser
A11.2.6	Seguridad de los equipos fuera de las instalaciones	SI	
A11.2.7	Reutilización o eliminación segura de equipos	SI	

			retirados de las funciones asociadas al rol.
A11.2.8	Equipo de usuario desatendido	SI	Se debe procurar que únicamente el responsable de un activo acceda a este o que se realice bajo la supervisión del mismo.
A11.2.9	Política de puesto de trabajo despejado y pantalla limpia	SI	
A12	**Seguridad de las operaciones**		
A12.1	**Procedimientos y responsabilidades operacionales**		
A12.1.1	Documentación de procedimientos operacionales	SI	Los procesos operacionales sobre los sistemas de información debe estar debidamente documentado
A12.1.2	Gestión de cambios	SI	
A12.1.3	Gestión de capacidades	SI	
A12.1.4	Separación de los recursos de desarrollo, prueba y operación	NO	No se realiza desarrollo de software de manera interna.
A12.2	**Protección contra el software malicioso (malware)**		
A12.2.1	Controles contra el código malicioso	SI	Imprescindible para evitar incidentes de SI
A12.3	**Copias de seguridad**		
A12.3.1	Copias de seguridad de la información	SI	Permitirán reestablecer la información en caso de una perdida de la misma en los activos
A12.4	**Registros y supervisión**		
A12.4.1	Registro de eventos	SI	

A12.4.2	Protección de la información del registro	SI	Es importante llevar un control de los eventos relacionados con los SI/TI, estos ayudarán en la toma de decisiones con respecto a la seguridad, la sincronización del reloj permitirá identificar con precisión la ocurrencia de los mismos.
A12.4.3	Registros de administración y operación	SI	
A12.4.4	Sincronización del reloj	SI	
A12.5	**Control del software en explotación**		
A12.5.1	Instalación del software en explotación	SI	Para evitar la filtración o perdida de información se debe garantizar que el software adquirido cumpla con los requisitos y el uso correcto de los mismos, solo debe ser instalado software de confianza y necesario en los procesos institucionales.
A12.6	**Gestión de la vulnerabilidad técnica**		
A12.6.1	Gestión de las vulnerabilidades técnicas	SI	Para evitar la filtración o perdida de información se debe garantizar que el software adquirido cumpla con los requisitos y las medidas de seguridad la su uso.
A12.6.2	Restricción en la instalación de software	SI	
A12.7	**Consideraciones sobre la auditoria de sistemas de información**		
A12.7.1	Controles de auditoría de sistemas de información	SI	
A13	**Seguridad de las comunicaciones**		
A13.1	**Gestión de la seguridad de las redes**		
A13.1.1	Controles de red	SI	

A13.1.2	Seguridad de los servicios de red	SI	La administración de la red debe ser eficaz y eficiente, para una mejor administración es necesario dividir las redes agregando los equipos según su uso.
A13.1.3	Segregación en redes	SI	
A13.2	**Intercambio de información**		
A13.2.1	Políticas y procedimientos de intercambio de información	SI	La implementación de mecanismos de seguridad frente al traspaso de información es de carácter fundamental.
A13.2.2	Acuerdos de intercambio de información	SI	
A13.2.3	Mensajería electrónica	SI	
A13.2.4	Acuerdos de confidencialidad o no revelación	SI	
A14	**Adquisición, desarrollo y mantenimiento de los sistemas de información**		
A14.1	**Requisitos de seguridad en los sistemas de información**		
A14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	SI	Esencial en el SGSI
A14.1.2	Asegurar los servicios de aplicaciones en redes públicas	SI	
A14.1.3	Protección de las transacciones de servicios de aplicaciones	SI	
A14.2	**Seguridad en el desarrollo y en los procesos de soporte**		
A14.2.1	Política de desarrollo seguro	NO	No se realiza desarrollo de software de manera interna.
A14.2.2	Procedimiento de control de cambios en sistemas	SI	Las actualizaciones, adaptaciones y modificaciones sobre los sistemas de
A14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	SI	

A14.2.4	Restricciones a los cambios en los paquetes de software	SI	información adquiridos son responsabilidad directa del proveedor.
A14.2.5	Principios de ingeniería de sistemas seguros	SI	
A14.2.6	Entorno de desarrollo seguro	NO	No se realiza desarrollo de software de manera interna.
A14.2.7	Externalización del desarrollo de software	SI	Es necesario garantizar que el software cumple con los requisitos funcionales y de seguridad previo a la implementación de los mismos.
A14.2.8	Pruebas funcionales de seguridad de sistemas	SI	
A14.2.9	Pruebas de aceptación de sistemas	SI	
A14.3	**Datos de prueba**		
A14.3.1	Protección de los datos de prueba	SI	
A15	**Relación con proveedores**		
A15.1	**Seguridad en las relaciones con proveedores**		
A15.1.1	Política de seguridad de la información en las relaciones con los proveedores	SI	En los contratos con los proveedores debe estar garantizada la seguridad de la información que gestionarán y la disponibilidad de los mismos
A15.1.2	Requisitos de seguridad en contratos con terceros	SI	
A15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	SI	
A15.2	**Gestión de la provisión de servicios del proveedor**		
A15.2.1	Control y revisión de la provisión de servicios del proveedor	SI	
A15.2.2	Gestión de cambios en la provisión del servicio del proveedor	SI	
A16	**Gestión de incidentes de seguridad de la información**		
A16.1	**Gestión de incidentes de seguridad de la información y mejoras**		
A16.1.1	Responsabilidades y procedimientos	SI	frente a los incidentes de seguridad el CISO, el comité de seguridad y cada uno
A16.1.2	Notificación de los eventos de seguridad de la información	SI	
A16.1.3	Notificación de puntos débiles de la seguridad	SI	

A16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	SI	de los responsables deben conocer el procedimiento a llevar frente a estos acontecimientos, mismos que deben ser comunicados de manera inmediata a los responsables de la seguridad de la información.
A16.1.5	Respuesta a incidentes de seguridad de la información	SI	
A16.1.6	Aprendizaje de los incidentes de seguridad de la información	SI	
A16.1.7	Recopilación de evidencias	SI	
A17	**Aspectos de seguridad de la información para la gestión de la continuidad de negocio**		
A17.1	**Continuidad de la seguridad de la información**		
A17.1.1	Planificación de la continuidad de la seguridad de la información	SI	Frente a acontecimientos adversos es necesario que exista un plan de contingencia para asegurar que se realicen al menos los procesos de carácter importante
A17.1.2	Implementar la continuidad de la seguridad de la información	SI	
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	SI	
A17.2	**Redundancias**		
A17.2.1	Disponibilidad de los recursos de tratamiento de la información	SI	Debe ser garantizada la disponibilidad de la información en todo momento que sea necesario.
A18	**Cumplimiento**		
A18.1	**Cumplimiento de los requisitos legales y contractuales**		
A18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	SI	Debe existir un respaldo legal sobre cada una de las políticas realizadas al
A18.1.2	Derechos de Propiedad Intelectual (DPI)	SI	
A18.1.3	Protección de los registros de la organización	SI	

A18.1.4	Protección y privacidad de la información de carácter personal	SI	igual que el proceso en casa de incumplimiento en ambas direcciones.
A18.1.5	Regulación de los controles criptográficos	SI	
A18.2	**Revisiones de la seguridad de la información**		
A18.2.1	Revisión independiente de la seguridad de la información	SI	
A18.2.2	Cumplimiento de las políticas y normas de seguridad	SI	
A18.2.3	Comprobación del cumplimiento técnico	SI	

Tabla 17: Declaración de aplicabilidad

Las existencias de todos estos documentos constituyen evidencias palpables de que el Sistema de Gestión está funcionando.

FASE 3: ANÁLISIS DE RIESGOS

En los apartados 6.1.2 y 8.2 de la norma ISO/IEC 27001 se establece que el análisis de riesgos es un requisito obligatorio para un Sistema Gestor de Seguridad de la Información, en la fase anterior de este documento se establece la metodología MAGERIT que describe el proceso para cumplir con lo estipulado en la norma y el mismo se efectúa a continuación.

3.1 ESTABLECIMIENTO DEL CONTEXTO

Según la metodología MAGERIT es necesario realizar el levantamiento de los activos de información de todos los departamentos de la UESMA, clasificarlos como primarios o de infraestructura y asignarlos a un responsable para posteriormente analizar los factores que ponen en riesgo a los mismos y así luego fijar controles para evitar el mal funcionamiento de los mismos y establecer un PCN. Este proceso es un punto crítico del SGSI puesto que de realizarse uno de los procesos anteriormente descritos puede conllevar a que se implemente un plan de seguridad ineficiente y se deberá retomar esta actividad lo cual implica pérdida de recursos para la institución.

3.2 INVENTARIO DE LOS ACTIVOS

Entiéndase por activo de información a todo componente o función que genera valor a los procesos de las actividades de la UESMA y pueden estar clasificados como Hardware (HW), Software (SW), Instalaciones (I), Datos/Información (D), Redes de Comunicación (COM), Servicios (S), Soporte de Información (SPI), Auxiliar (AUX),

Personal (P). En la UESMA se obtienen los siguientes resultados de acuerdo al inventario de activos.

Para establecer la prioridad de los activos a parte de funcionamiento es importante valorar a cada uno de ellos de acuerda a las inversiones realizadas en la institución y para ello se usará la siguiente tabla.

Acrónimo	Valoración Cualitativa	Rango
MA	Muy Alta	X > 100.000
A	Alta	50.000 < x > 100.000
M	Media	10.000 < x > 50.000
B	Baja	5.000 < x > 10.000
MB	Muy Baja	X < 5.000

Tabla 18: Valoración de activos

Con respecto a las dimensiones los activos se pueden clasificar por su:

- **Confidencialidad (C):** La información no es revelada ni accedida por personas o procesos no autorizados.
- **Integridad (I):** El activo no debe haber sido alterado sin autorización.
- **Disponibilidad (D):** El activo puede ser accedido cuando es necesario por el personal autorizado.
- **Autenticidad (A):** Se garantizan la procedencia de los datos.
- **Trazabilidad (T):** Identificar quien y como usa el activo.

Estas características deben ser evaluadas de acuerdo a una valoración de daño posible de los activos, es decir, analizar la criticidad de estos y las consecuencias al producirse un incidente en la seguridad y para esto se establecen los siguientes valores propuestos por la metodología MAGERIT:

Escala	Valoración	Criterios
10	Extremo	Daño extremadamente grave.
8-9	Muy Alto	Daño muy grave.
6-7	Alto	Daño grave.
4-5	Medio	Daño considerable.

2-3	Bajo	Daño menor.
1	Despreciable	Daño irrelevante.

Tabla 19: Valores de criticidad de los activos

Para tener una percepción clara de las incidencias o dependencias sobre otros activos es importante saber que los activos superiores o primarias dependen del valor de criticidad de los inferiores, lo cual provoca que la criticidad de un resultado acumulativo, y conocer la cadena de afectaciones, a continuación, se describen las dependencias entre los activos:

a) El funcionamiento del Hardware (HW) depende de las Instalaciones (I), de ciertos elementos de Comunicación (COM) y del abastecimiento de energía eléctrica (AUX)

b) El Software (SW) depende directamente del Hardware (HW).

c) Los Datos/Información dependen del Hardware (HW) y del Software (SW).

d) Los Servicios dependen del Hardware (HW), del Software (SW), de las Comunicaciones (COM) y las Instalaciones (I).

e) Las Comunicaciones (COM) dependen del Hardware (HW), las Instalaciones (I) y del abastecimiento eléctrico (AUX).

f) Los soportes de información (SI) dependen de las Instalaciones (I) dependiendo del activo que se use (AUX)

g) Auxiliares (AUX) dependen de las instalaciones (I), del Hardware (HW) y de otros elementos Auxiliares (AUX)

h) Las Instalaciones (I) no tienen dependencias.

i) Personal (P) no tiene dependencias.

Una vez descritas todas las dependencias y valoraciones se proceden a definir la valoración de los activos, así como la identificación de los mismos y de responsables sobre los mismos.

TIPO	ID	Cantidad	ACTIVO	VALOR	DEPENDENCIAS	CRITICIDAD				
						C	I	D	A	T
HW	HW1	3	Servidor	A	I1 - COM1 - AUX1 - AUX2	10	9	10	9	9
	HW2	1	Router	B	I1 - COM1 - AUX1 - AUX2	9	6	7	6	8
	HW3	9	Switch	B	I1 - COM1 - AUX1 - AUX2	4	3	8	4	6

	HW4	248	Computador de escritorio	MA	I2 - I3 - COM1 - AUX1 - AUX2	5	6	7	5	8
	HW5	43	Laptop	M	AUX1 - AUX2 - COM5	7	5	6	4	7
	HW6	2	Copiadora	B	AUX1 - I2	1	3	5	5	7
	HW7	18	Impresoras	B	I2 - AUX1	2	2	4	3	3
	HW8	23	Teléfono IP	MB	I2 - COM2 - COM-3 - AUX1 - AUX2	7	8	5	6	5
	HW9	22	Repetidores WIFI	MB	I1 - AUX1 - AUX2 - COM2	6	5	2	4	7
	HW10	1	Impresora de credenciales	B	AUX1	1	2	3	1	2
SW	SW1	1	Firewall Endian Comunity	MB	HW1	6	8	8	6	8
	SW2	3	Windows Server 2012	MB	HW1	8	9	9	9	9
	SW3	291	Windows 10 PRO	MB	HW4 - HW5	3	4	5	4	5
	SW4	291	Microsoft Office 2016	MB	HW4 - HW5	3	4	5	4	5
	SW5	216	NetSupportSchool	MB	HW4	1	2	2	3	4
	SW6	1	Prosoft Edu	B	COM1	7	10	9	9	8
I	I1	1	DATA CENTER	MA	-	10	9	10	8	7
	I2	16	Oficinas	A	-	7	8	8	8	7
	I3	6	Laboratorio para estudiantes	MA	-	1	2	6	2	4
	I4	2	Taller técnico	A	-	6	-	3	-	6
D	D1		Contratos	M	HW4 - COM1	10	10	8	10	8
	D2		Datos académicos de estudiantes	M	HW4 - HW5 - COM1	7	8	8	9	7
	D3		Datos financieros	MA	HW1 - HW4 - HW5 - AUX1 - AUX2	8	10	9	10	9
	D4		Datos de empleados	M	HW1 - HW4 - AUX1 - AUX2 - COM1	7	8	8	9	7
	D5		Reglas del firewall	A	SW1	6	9	9	7	7
COM	COM1	1	Conexión al ISP	B	I1 - HW1 - SW1 - AUX1 -AUX2	7	8	7	6	6
	COM2	12	VLAN	MB	I1 - HW3 - COM1	7	6	7	5	6
	COM3	1	Troncal telefónica	MB	I1 - AUX1	2	1	7	4	5
	COM4	1	Circuito de cámaras de seguridad	B	I1 - I2 - I3 - I4 - AUX1 - AUX2	6	4	6	5	7
	COM5	1	Red Inalámbrica	MB	HW1 - HW3 - HW9 - SW2	7	6	7	5	6
S	S1	5	Servicios internos	M	I1 - I2 - I3 - I4 - AUX1 - AUX2 - COM2 - COM5	7	7	8	7	7
	S2	3	Servicios terceras partes	B	COM1 - HW4 - HW5	7	7	8	8	7
SP	SPI1	10	Discos duros externos	MB	HW4 - HW5	6	8	7	7	7

	SPI2	100	Memorias USB	MB	HW4 - HW5	6	8	7	7	7
	SPI3	24	Proyector	B	HW4 - HW5 - AUX1	-	-	6	2	3
	SPI4	30	Lector DVD externo	MB	HW4 - HW5	-	-	5	-	6
AUX	AUX1	1	Cableado de suministro eléctrico	A	I1 - I2 - I3 - I4	-	-	10	-	-
	AUX2	1	Cableado de red LAN	A	I1 - I2 - I3 - I4 - AUX1	-	-	10	-	-
	AUX3	20	Extintores	B	I1 - I2 - I3 - I4	-	-	1	-	-
	AUX4	23	Acondicionadores de aire	A	I1 - I2 - I3 - I4 - AUX1	-	-	7	-	-
P	P1	1	Director de comunidad	MA	-	-	-	-	-	-
	P2	1	Coordinador general	MA	-	-	-	-	-	-
	P3	3	Mandos intermedios	MA	-	-	-	-	-	-
	P4	8	Responsable de áreas	MA	-	-	-	-	-	-
	P5	120	Docentes	MA	-	-	-	-	-	-
	P6	45	Personal auxiliar y de servicios	MA	-	-	-	-	-	-

Tabla 20: Inventario de activos y valoración según varios criterios

El alcance del presente Sistema Gestor de Seguridad de la Información está contemplado a todos los procesos relacionados con la seguridad de los sistemas de información, es por ello que se ha tomado también los activos relacionados con estos procesos en esta fase de análisis de riesgos. Para entender de mejor manera se procede a realizar una breve y concisa explicación de la tabla 19.

3.2.1 HARDWARE (HW)

En este apartado entran todos los elementos físicos relacionados con los sistemas de información y se detallan:

1. 3 Servidores: (HW1)
    a. HP Proliant DL320e Gen8 v2.
    b. HP Proliant DL360e Gen8.
    c. HP Proliant DL380 Gen10
2. 1 Router: CISCO SG300-28 (HW2)
3. 9 Switch: CISCO SG200-50 (HW3)
4. 248: Computadores de escritorio: Placa Madre Asus, RAM DDR3 8GB, Procesador I5, SDD 240GB, Monitor AOC 19.5”, Combo Case Microsoft (HW4)
5. 43 Laptop: (HW5)
    a. 22 DELL Inspiron 14 3000 Series.
    b. 21 DELL Inspiron 3480 Series.
6. 2 Copiadoras: RICOH MPC 4501 (HW6)
7. 18 Impresoras: Epson L4150 (HW7)

8. 23 Telefonos IP: Grandstream GXP 1405 (HW8)
9. 22 Repetidores WIFI: (HW9)
    a. 10 Platos Ubiquiti UAP-AC Dual Band
    b. 12 Antenas Ubiquiti Mesh Dual Band Outdoor
10. Impresora de credenciales: ZEBRA ZC 300. (HW10)

3.2.2 SOFTWARE. (SW)

Son todos los sistemas operativos y aplicaciones.

1. Firewall Endian (SW1): Controla el acceso de todos los dispositivos a la red y administra la conexión a internet.

2. Windows Server 2012: (SW2)

    a. Se encuentra el servicio de DHCP y la aplicación de control de asistencia del personal de la institución.

    b. Se encuentra el servicio UNIFI que permite administrar la red inalámbrica.

    c. Se encuentra el servicio contable con toda la información financiera y tributaria de la institución.

3. 291 Windows 10 PRO: Es el sistema operativo usado en las computadoras de escritorio y portátiles. (SW3)

4. 291 Microsoft Office 2016: El paquete ofimático usado en las computadoras de escritorio y portátiles. (SW4)

5. 216 NetSupportSchool: Aplicación tipo cliente-servidor usada para control de uso de equipos en los laboratorios de computación. (SW5)

6. 1 Prosoft Edu: Sistema de gestión académica (SW6)

3.2.3 INSTALACIONES (I)

1. DATA CENTER: Centro de procesamiento de datos. (I1)

2. 15 Oficinas: Departamentos de la institución (I2)

    a. Dirección de comunidad
    b. Rectorado
    c. Vicerrectorado
        a. Académico
        b. Administrativo
    d. TIC

e. Contabilidad
f. Economato
g. GTH
h. Pastoral
i. Secretaría
j. Recepción
k. Garita
l. Taller de Mecánica
m. Taller de electrónica.
n. Bodega.

3. 6 Laboratorios para estudiantes
    a. Laboratorio 1.
    b. Laboratorio 2.
    c. Laboratorio 3.
    d. Laboratorio 4.
    e. Laboratorio de soporte técnico.
    f. Laboratorio de redes.
4. 2 Talleres técnicos: Espacios dedicados a las prácticas en las áreas técnicas.
    a. Electrónica.
    b. Mecánica.

3.2.4 DATOS / INFORMACIÓN (D)

1. Contratos: Son todos los documentos legales por contratación de servicios. (D1)
2. Datos académicos de estudiantes: Toda la información personal y pedagógica de los estudiantes. (D2)
3. Datos financieros: Toda información económica de la institución como cuentas por cobrar, cuentas por pagar, escalafones de sueldo, conciliaciones bancarias e información tributaria. (D3)
4. Datos de empleados: Es toda la información personal y laboral del personal bajo relación de dependencia de la UESMA. (D4)
5. Reglas del firewall: Son todas aquellas configuraciones, reglas y demás parámetros establecidos en el firewall para el control de la red insititucional.

3.2.5 COMUNICAION (COM)

1. Conexión al ISP: Enlace al proveedor del servicio de internet, en el caso particular de la UESM la empresa que presta este servicio es Netlife. (COM1)

2. 11 VLAN: Virtual LAN, son configuraciones realizadas en router y switches con el fin de segmentar y administrar de mejor manera los equipos que se encuentran en la red, y estas VLAN son: (COM2)

   a. Servidores.
   b. Administrativos.
   c. Lab1
   d. Lab2
   e. Lab3
   f. Lab4
   g. Lab5
   h. Contabilidad
   i. DECE
   j. WIFI_Comunidad
   k. WIFI_Profesores
   l. Cámaras de seguridad

3. Troncal telefónica: Dispositiva que administra las llamadas telefónicas interna y externas. (COM3)

4. Circuito de cámaras de seguridad: Red de dispositivos que hacen posible la video vigilancia dentro de la institución y su perímetro externo. (COM4).

5. Red inalámbrica: Conjunto de dispositivos tendidos de manera estratégica en toda la institución que permiten replicar la señal de la red inalámbrica para que los dispositivos se conecten a la red de la institución (COM5)

3.2.6 SERVICIOS (S)

1. Servicios internos: Son sistemas que administran varios elementos y hacen posible la disponibilidad de un servicio. (S1)
   a. Servicio de gestión académica.
   b. Servicio de facturación electrónica
   c. Alojamiento de la página web
2. Servicios terceras partes: Son todos aquellos servicios en los cuales intervienen otras entidades o empresas contratadas por la UESMA para suplir distintas necesidades momentáneas (SPI2)
   a. Mantenimiento de la red eléctrica.
   b. Mantenimiento y adecuación de las instalaciones.
   c. Mantenimiento de los acondicionadores de aire.

3.2.7 SOPORTES INFORMÁTICOS (SPI)

1. 10 Discos duros externos: Dispositivo de almacenamiento masivo portátil, usado para guardar información que no es posible mantener en los equipos por saturación de espacio o por sensibilidad de la misma. (SP13)
2. 100 Memorias USB: Dispositivos de 16gb de almacenamiento que permiten extraer información de ordenadores u otros servicios e introducirla en otros, generalmente se almacena información rápida y sencilla que se necesita fácil acceso. (SP14)
3. 24 Proyector: Dispositivo óptico que replica imágenes para que sean mejor apreciada en espacios grandes donde no abastece la pantalla del equipo habitual. (SP15)
4. 30 Lector de DVD: Dispositivos portátiles que permiten a través de puerto usb cargar la información contenida en un CD a los ordenadores que no tienen un lector incorporado. (SP16)

3.2.7 AUXILIARES (AUX)

1. Cableado de suministro eléctrico: Son todos los componentes que hacen posible que los dispositivos que necesitan energía eléctrica para funcionar lo hagan. (AUX1)
2. Cableado de red LAN: Elementos que hacen posible la comunicación entre los dispositivos internos de la institución y hacia el internet. (AUX2)
3. Extintores: Es un equipo que sirve para apagar fuegos mediante un componente que repele incendios. (AUX3)
4. Acondicionadores de aire: Equipo que modifica la temperatura del ambiente para producir una adecuada según el entorno donde se encuentre. (AUX4)

3.2.8 PERSONAL (P)

- ✓ Director de la comunidad: Máxima autoridad de la institución, ver ilustración 2.
- ✓ Coordinador general: Responsable de la administración general de la UESMA.
- ✓ 7 Mandos intermedios: Responsables de distintas áreas que forman parte de los directivos de la institución,
    a. Director de pastoral
    b. Rector.
    c. Vicerrector Académico.
    d. Vicerrector Administrativo.
- ✓ Responsables de áreas: Son las personas responsables de coordinar las distintas áreas que forman parte de la institución, llamados también jefes departamentales.
    a. Coordinador de TIC.
    b. Coordinador de GTH.
    c. Coordinador de DPEI.
    d. Coordinador de pastoral.
    e. Coordinador de DECE.

f. Coordinador de taller.

h. Coordinador de contabilidad.

i. Coordinador de Bodega.

6. 120 Docentes: Profesionales de la educación que imparten sus conocimientos en los distintos espacios destinados para este proceso.
7. 45 Personal auxiliar y de servicios: Personas responsables del mantenimiento sanitario y servicios adicionales propios de la institución.

3.3 ANALISIS DE RIESGOS.

3.3.1 IDENTIFICACIÓN DE AMENAZAS.

La metodología de análisis de riesgos MAGERIT en el apartado 5 referente a las amenazas establece la siguiente clasificación de las mismas.

1. **Desastres Naturales (N):** Sucesos que hacen referencia a pérdidas materiales o de vidas humanas sin la intervención directa de las personas.
    a. Fuego (N1).
    b. Daños por agua N2.
    c. Desastres naturales N*.
2. **Desastres industriales (I):** Sucesos repentinos que ocasionan deficiencia en la producción de una empresa, estos pueden provocarse de manera accidental o deliberada, pero siempre está relacionado al descuido o intención de las personas.
    a. Fuego (I1).
    b. Daño por agua (I2).
    c. Desastres industriales (I*).
    d. Contaminación mecánica (I3).
    e. Contaminación electromagnética (I4).
    f. Avería de origen físico o lógico (I5).
    g. Corte de suministro eléctrico (I6).
    h. Condiciones inadecuadas de temperatura o humedad (I7).
    i. Fallo de servicio de comunicaciones (I8).
    j. Interrupción de otros servicios y suministros esenciales (I9).
    k. Degradación de los soportes de almacenamiento de la información (I10).
    l. Emanaciones electromagnéticas (I11).
3. **Errores y fallos no intencionales (E):** Fallos no intencionales causados por las personas.
    a. Errores de los usuarios (E1).
    b. Errores del administrador (E2).
    c. Errores de monitorización, log (E3).
    d. Errores de configuración (E4).

e. Deficiencias en la organización (E7).
f. Difusión de software dañino (E8).
g. Errores de [re-]encaminamiento (E9).
h. Errores de secuencia (E10).
i. Alteración accidental de la información (E15).
j. Destrucción de la información (E18).
k. Fugas de información (E19).
l. Vulnerabilidades de los programas (software) (E20).
m. Errores de mantenimiento / actualización de programas (software) (E21).
n. Errores de mantenimiento / actualización de equipos (hardware) (E23).
o. Caída del sistema por agotamiento de recursos (E24).
p. Perdida de equipos (E25).
q. Indisponibilidad del personal (E28).

4. Ataques intencionados (A)
   a. Manipulación de los registros de actividad (log) (A3).
   b. Manipulación de la configuración (A4).
   c. Suplantación de la identidad del usuario (A5).
   d. Abuso de privilegios de acceso (A6).
   e. Uso no previsto (A7).
   f. Difusión de software dañino (A8).
   g. [Re-]encaminamiento de mensajes (A9).
   h. Alteración de secuencia (A10).
   i. Acceso no autorizado (A11).
   j. Análisis de tráfico (A12).
   k. Repudio (A13).
   l. Interceptación de información (escucha) (A14).
   m. Modificación deliberada de la información (A15).
   n. Destrucción de información (A18).
   o. Divulgación de información (A19).
   p. Manipulación de programas (A22).
   q. Manipulación de los equipos (A23).
   r. Denegación de servicio (A24).
   s. Robo (A25).
   t. Ataque destructivo (A26)
   u. Ocupación enemiga (A27)
   v. Indisponibilidad del personal (A28)
   w. Extorsión (A29)
   x. Ingeniería social (picaresca) (A30)

Es necesario tener en cuenta la frecuencia con la que una amenaza puede materializarse para un mejor análisis, la tabla a continuación muestra la frecuencia basado en un año calendario no bisiesto.

FRECUENCIA	ID_FRECUENCIA	RANGO	VALOR
Muy Alta	FMA	Diaria	100
Alta	FA	Quincenal	10
Media	FM	Bimensual	1
Baja	FB	Semestral	0.1
Muy Baja	FMB	Anual	0.01

Tabla 21: Frecuencia de amenazas

3.3.2 IMPACTO POTENCIAL

MAGERIT denomina impacto potencial a la medida del daño sobre el activo derivado de la materialización de una amenaza, teniendo claro el valor de los activos en las distintas dimensiones ya mencionadas y la degradación que ocasionan la amenazas, es necesario derivar el impacto de estas sobre los sistemas.

Calculo del impacto potencial

Para realizar este cálculo se define el porcentaje del valor del activo que se pierde en el caso de que ocurra un incidente que afecte a este, la siguiente tabla muestra los porcentajes dependiendo el impacto para luego proceder a asignarlo según las dependencias a los activos.

IMPACTO	VALOR
Muy Alto	100%
Alto	75%
Medio	50%
Bajo	25%
Muy Bajo	5%

Tabla 22: Valoración de impacto

La tabla de impacto potencial está conformada por varios elementos, el de criticidad es el mismo usado en la tabla 19, mientras que el % IMPACTO es la asignación que se asigna en cada dependencia a cada activo y los valores están la tabla de valoración de impacto, el producto de estas dos mencionadas es el % IMPACTO POTENCIAL.

TIPO	ID_ACT	VALOR	CRITICIDAD					% IMPACTO					% I POTENCIAL				
			C	I	D	A	T	C	I	D	A	T	C	I	D	A	T
HW	HW1	A	10	9	10	9	9	100%	50%	100%			10	4.5	10	0	0
	HW2	B	9	6	7	6	8	100%	75%	100%	-	-	9	4.5	7	0	0
	HW3	B	4	3	8	4	6	100%	75%	100%	-	-	4	2.3	8	0	0
	HW4	MA	5	6	7	5	8	75%	25%	75%	-	-	3.8	1.5	5.3	0	0
	HW5	M	7	5	6	4	7	75%	25%	75%	-	50%	5.3	1.3	4.5	0	3.5
	HW6	B	1	3	5	5	7	75%	25%	50%	-	-	0.8	0.8	2.5	0	0
	HW7	B	2	2	4	3	3	75%	25%	75%	-	-	1.5	0.5	3	0	0
	HW8	MB	7	8	5	6	5	75%	75%	75%	-	50%	5.3	6	3.8	0	2.5
	HW9	MB	6	5	2	4	7	25%	75%	75%	-	75%	1.5	3.8	1.5	0	5.3
	HW10	B	1	2	3	1	2	5%	5%	25%	-	-	0.1	0.1	0.8	0	0
SW	SW1	MB	6	8	8	6	8	100%	75%	100%	-	-	6	6	8	0	0
	SW2	MB	8	9	9	9	9	100%	100%	75%	75%	-	8	9	6.8	6.8	0
	SW3	MB	3	4	5	4	5	100%	100%	50%	75%	-	3	4	2.5	3	0
	SW4	MB	3	4	5	4	5	100%	75%	75%	75%	-	3	3	3.8	3	0
	SW5	MB	1	2	2	3	4	25%	50%	50%	-	25%	0.3	1	1	0	1
	SW6	B	7	10	9	9	8	100%	100%	100%	100%	75%	7	10	9	9	6
I	I1	MA	10	9	10	8	7	50%	50%	100%	-	-	5	4.5	10	0	0
	I2	A	7	8	8	8	7	50%	50%	100%	-	-	3.5	4	8	0	0
	I3	MA	1	2	6	2	4	50%	50%	75%	-	-	0.5	1	4.5	0	0
	I4	A	6	-	3	-	6	50%	50%	75%	-	-	3	0	2.3	0	0
D	D1	M	10	10	8	10	8	100%	75%	50%	100%	100%	10	7.5	4	10	8
	D2	M	7	8	8	9	7	75%	75%	50%	100%	100%	5.3	6	4	9	7
	D3	MA	8	10	9	10	9	100%	75%	50%	100%	100%	8	7.5	4.5	10	9
	D4	M	7	8	8	9	7	75%	75%	50%	100%	100%	5.3	6	4	9	7
	D5	A	6	9	9	7	7	75%	50%	100%	75%	75%	4.5	4.5	9	5.25	5.25

COM	COM1	B	7	8	7	6	6	75%	25%	100%	100%	-	5.3	2	7	6	0
	COM2	MB	7	6	7	5	6	75%	100%	100%	75%	-	5.3	6	7	3.8	0
	COM3	MB	2	1	7	4	5	50%	25%	75%	100%	-	1	0.3	5.3	4	0
	COM4	B	6	4	6	5	7	50%	25%	75%	75%	-	3	1	4.5	3.8	0
	COM5	MB	7	6	7	5	6	75%	100%	100%	75%	-	5.3	6	7	3.8	0
SPI	S1	M	7	7	8	7	7	100%	75%	100%	75%	100%	7	5.3	8	5.3	7
	S2	B	7	7	8	8	7	75%	50%	75%	50%	75%	5.3	3.5	6	4	5.3
	SPI1	MB	6	8	7	7	7	50%	75%	75%	50%	-	3	6	5.3	3.5	0
	SPI2	MB	6	8	7	7	7	50%	50%	100%	-	-	3	4	7	0	0
	SPI3	B	-	-	6	2	3	5%	25%	75%	-	50%	0	0	4.5	0	1.5
	SPI4	MB	-	-	5	-	6	5%	5%	50%	-	25%	0	0	2.5	0	1.5
AUX	AUX1	A	-	-	10	-	-	50%	50%	100%	-	-	0	0	10	0	0
	AUX2	A	-	-	10	-	-	50%	50%	100%	-	-	0	0	10	0	0
	AUX3	B	-	-	1	-	-	50%	25%	75%	-	-	0	0	0.8	0	0
	AUX4	A	-	-	7	-	-	50%	50%	75%	-	-	0	0	5.3	0	0
P	P1	MA	-	-	6	-	-	50%	25%	75%	-	-	0	0	4.5	0	0
	P2	MA	-	-	5	-	-	50%	25%	75%	-	-	0	0	3.8	0	0
	P3	MA	-	-	4	-	-	50%	25%	50%	-	-	0	0	2	0	0
	P4	MA	-	-	3	-	-	50%	50%	100%	-	-	0	0	3	0	0
	P5	MA	-	-	2	-	-	25%	50%	50%	-	-	0	0	1	0	0
	P6	MA	-	-	1	-	-	25%	25%	50%	-	-	0	0	0.5	0	0

Tabla 23: Valoración de impacto comercial

3.3.3 RIESGO ACEPTABLE.

El riesgo aceptable es la inseguridad sobre los activos que es posible para la empresa asumir, esto se hace cuando no es rentable ni factible reducir la posibilidad de materialización de una amenaza y se procede a minimizar las consecuencias a niveles aceptables para la UESMA, sin que esto sea un perjuicio muy grave en todos los niveles: logístico, económico, credibilidad, etc. Este es el producto de la frecuencia por el impacto potencial.

3.3.4 RIESGO RESIDUAL.

Es el nivel de riesgo que permanece en la organización tras mitigar/reducir o eliminar los riesgos, exige que se tomen medidas previas para que, de manifestarse, su efecto sea de mínimo impacto para la institución.

TIPO	ID_ACTIVO	VALOR	FRECUENCIA		% I POTENCIAL					RIESGO				
			Num.	Cual.	C	I	D	A	T	C	I	D	A	T
HW	HW1	A	0.1	FB	10	4.5	10	0	0	1	0.45	1	0	0
	HW2	B	0.1	FB	9	4.5	7	0	0	0.9	0.45	0.7	0	0
	HW3	B	0.1	FB	4	2.3	8	0	0	0.4	0.23	0.8	0	0
	HW4	MA	10	FA	3.8	1.5	5.3	0	0	37.5	15	52.5	0	0
	HW5	M	10	FA	5.3	1.3	4.5	0	3.5	52.5	12.5	45	0	35
	HW6	B	0.01	FMB	0.8	0.8	2.5	0	0	0.01	0.01	0.03	0	0
	HW7	B	0.01	FMB	1.5	0.5	3	0	0	0.02	0.01	0.03	0	0
	HW8	MB	0.1	FB	5.3	6	3.8	0	2.5	0.53	0.6	0.38	0	0.25
	HW9	MB	1	FM	1.5	3.8	1.5	0	5.3	1.5	3.75	1.5	0	5.25
	HW10	B	0.01	FMB	0.1	0.1	0.8	0	0	0	0	0.01	0	0
SW	SW1	MB	1	FM	6	6	8	0	0	6	6	8	0	0
	SW2	MB	10	FA	8	9	6.8	6.8	0	80	90	67.5	67.5	0
	SW3	MB	1	FM	3	4	2.5	3	0	3	4	2.5	3	0
	SW4	MB	1	FM	3	3	3.8	3	0	3	3	3.75	3	0
	SW5	MB	1	FM	0.3	1	1	0	1	0.25	1	1	0	1
	SW6	B	10	FA	7	10	9	9	6	70	100	90	90	60
I	I1	MA	1	FM	5	4.5	10	0	0	5	4.5	10	0	0
	I2	A	1	FM	3.5	4	8	0	0	3.5	4	8	0	0
	I3	MA	1	FM	0.5	1	4.5	0	0	0.5	1	4.5	0	0
	I4	A	1	FM	3	0	2.3	0	0	3	0	2.25	0	0
D	D1	M	1	FM	10	7.5	4	10	8	10	7.5	4	10	8

	D2	M	10	FA	5.3	6	4	9	7	52.5	60	40	90	70
	D3	MA	1	FM	8	7.5	4.5	10	9	8	7.5	4.5	10	9
	D4	M	1	FM	5.3	6	4	9	7	5.25	6	4	9	7
	D5	A	1	FM	5.3	6	4	9	7	0.525	0.6	0.4	0.9	0.7
COM	COM1	B	10	FA	5.3	2	7	6	0	52.5	20	70	60	0
	COM2	MB	0.1	FB	5.3	6	7	3.8	0	0.53	0.6	0.7	0.4	0
	COM3	MB	0.1	FB	1	0.3	5.3	4	0	0.1	0.1	0.5	0.4	0
	COM4	B	1	FM	3	1	4.5	3.8	0	3	1	4.5	3.8	0
	COM5	MB	1	FM	5.3	6	7	3.8	0	5.25	6	7	3.8	0
S	S1	M	10	FA	7	5.3	8	5.3	7	70	52.5	80	52.5	70
	S2	B	1	FM	5.3	3.5	6	4	5.3	5.25	3.5	6	4	5.25
SPI	SPI1	MB	10	FA	3	6	5.3	3.5	0	30	60	52.5	35	0
	SPI2	MB	100	FMA	3	4	7	0	0	300	400	700	0	0
	SPI3	B	0.1	FB	0	0	4.5	0	1.5	0	0	0.45	0	0.15
	SPI4	MB	0.01	FMB	0	0	2.5	0	1.5	0	0	0.03	0	0.02
AUX	AUX1	A	10	FA	0	0	10	0	0	0	0	100	0	0
	AUX2	A	1	FM	0	0	10	0	0	0	0	10	0	0
	AUX3	B	0.1	FB	0	0	0.8	0	0	0	0	0.08	0	0
	AUX4	A	1	FM	0	0	5.3	0	0	0	0	5.25	0	0
P	P1	MA	0.1	FB	0	0	4.5	0	0	0	0	0.45	0	0
	P2	MA	0.1	FB	0	0	3.8	0	0	0	0	0.38	0	0
	P3	MA	0.1	FB	0	0	2	0	0	0	0	0.2	0	0
	P4	MA	1	FM	0	0	3	0	0	0	0	3	0	0
	P5	MA	10	FA	0	0	1	0	0	0	0	10	0	0
	P6	MA	10	FA	0	0	0.5	0	0	0	0	5	0	0

Tabla 24: Valoración de riesgo aceptable y residual.

Según el informe del comité se seguridad se establece el nivel aceptable es menor a 50, por lo tanto, todas aquellas valoraciones por encima de este nivel deberán ser tratadas para disminuir su riesgo por debajo de los 50 de manera inmediata, también se resaltan valores entre 30 y 49 de valoración para que sean considerado posteriormente y procurar que sobrepase el nivel. Teniendo en cuenta estos parámetros se establecen 29 dependencias en los activos en nivel crítico y 6 en un nivel que debe ser tomado en cuenta para su proximidad al umbral de riesgo aceptable

3.4 CONCLUSIONES

3.4.1 DE LOS RIESGOS

A continuación, se presenta una tabla que permite identificar los activos en riesgos con la dependencia con valores críticos (50 o mayor) y la que se encuentra en un nivel considerable de tratamiento (30 a 49). Es ineludible recalcar que los activos con dependencia con riesgo por encima de 50 son los que deben ser tratados de manera inmediata para llevar el riesgo a un nivel aceptable. De acuerdo al riesgo acumulado únicamente considerando los valores que cumplen las condiciones descritas se ordenan desde el que tiene el riesgo más crítico hasta el menos crítico para de acuerdo a esta lista dar tratamiento al riesgo.

ID_ACTIVO	ACTIVO	VALOR	RIESGO				
			C	I	D	A	T
HW4	Computador de escritorio	MA	37.5		52.5		
AUX1	Cableado de suministro eléctrico	A		0	100		
S1	Servicios internos	M	70	52.5	80	52.5	70
HW5	Laptop	M	52.5		45	0	35
SPI2	Memorias USB	MB	300	400	700		
SW6	Prosoft Edu	B	70	100	90	90	60
COM1	Conexión al ISP	B	52.5		70	60	
SPI1	Discos duros externos	MB	30	60	52.5	35	
SW2	Windows Server 2012	MB	80	90	67.5	67.5	
D2	Datos académicos de estudiantes	M	52.5	60	40	90	70

Tabla 25: Activos en estado de riesgo.

3.4.2 DE LAS AMENAZAS

En la ilustración es posible apreciar la representación de las vulnerabilidades tratadas en esta fase, por cada activo en riesgo se encuentra la representación de las dimensiones que cumplen el requisito para que se realice el respectivo tratamiento de riesgo.

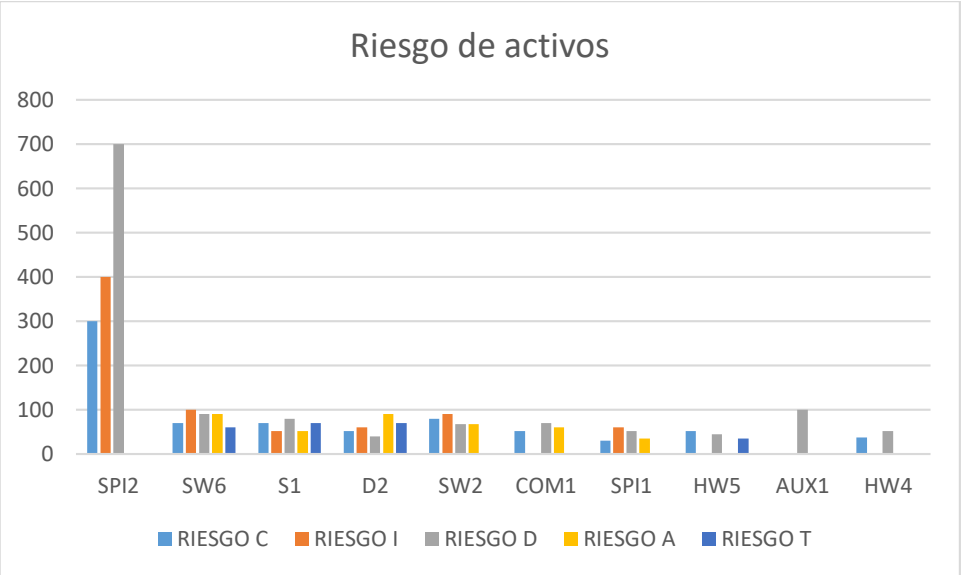

Ilustración 11: Presencia de amenazas por dependencias.

De la ilustración anterior se puede concluir que las amenazas tienen la misma representatividad en el hardware (HW), software (SW) y los soportes, ordenados por prioridad tal como se los menciona considerando el valor de los activos y la importancia en los procesos de la institución.

- La dependencia con mayor representación, 8 para ser precisos, es la de disponibilidad (D), esto quiere decir que la mayoría de amenazas ponen en riesgo el uso de los activos.
- Los activos con riesgo en la dependencia de confiabilidad (C), que son 8 apariciones, tienden a caer en manos de personas a las cuales no estaba dirigida la información.
- Con 6 representaciones se encuentra la dependencia de integridad (I), por lo cual los activos con este riesgo son propensos a que la información que contiene está expuesta y puede ser modificada de manera diferente a la información original.
- La autenticidad (A) que es una de las dependencias que se ven involucradas en riesgo con 5 apariciones mayores o iguales de 50 significa que los activos pueden ser accedidos por personas que no tienen autorización de acceso.
- Finalmente, con 3 apariciones está la dependencia de trazabilidad (T), en estos activos se ve en riesgo la verificación de la cadena de uso sobre los mismos.
- Las dependencias que están entre 30 y 49, es decir con proximidad al umbral de riesgo aceptable en total son 6, teniendo mayor incidencia en la disponibilidad de 2 activos y la menor es trazabilidad de 1 activo.

3.4.3 DEL RIESGO ACEPTABLE Y RESIDUAL.

En la ilustración # es apreciable la cantidad de riesgos por debajo del nivel aceptable establecido por el comité de seguridad de la información.

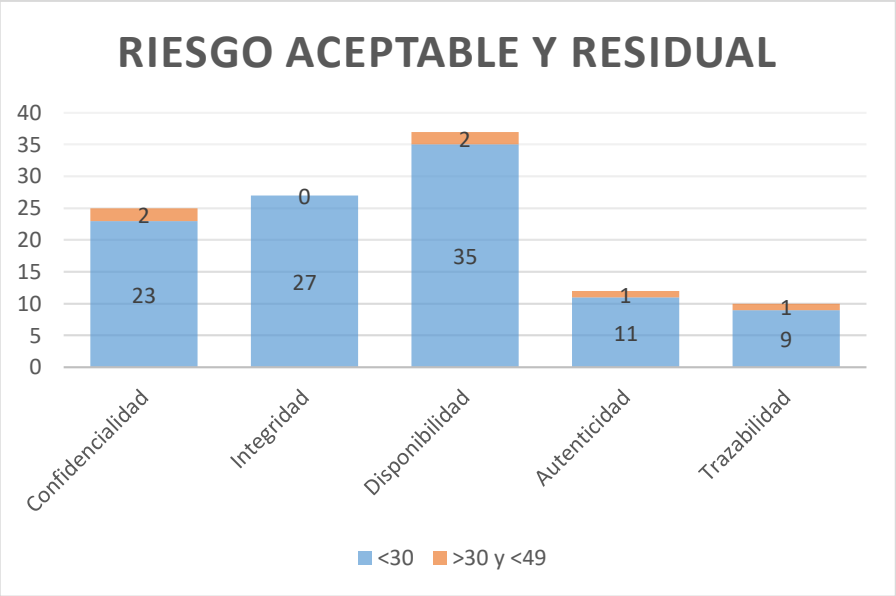

Ilustración 12: Riesgo aceptable y residual.

De la ilustración se puede concluir que existen un total de 201 riesgos de 230 en un nivel considerado aceptable o inexistente, de estos, constan 6 en el nivel que se establece que debe ser tratado el riesgo para evitar llegue a un nivel crítico.

3.4.4 GENERALES

Las gráficas a continuación permitirán ilustrar la media aritmética obtenida en cada dependencia por cada tipo de activo.

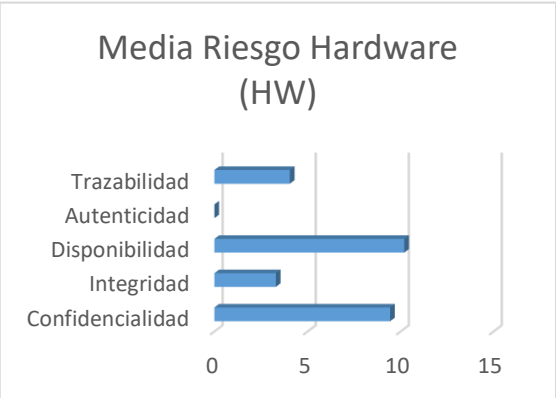

Ilustración 13: Media de riesgos en el hardware.

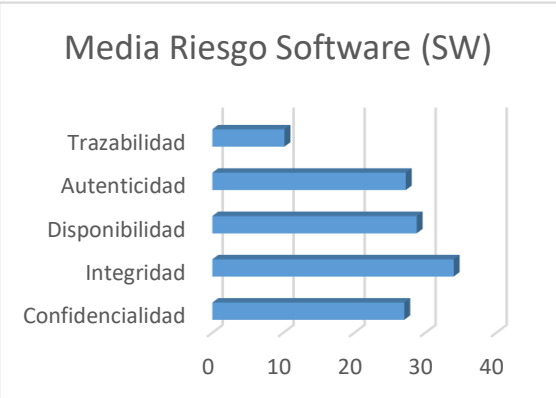

Ilustración 14: Media de riesgos en el software.

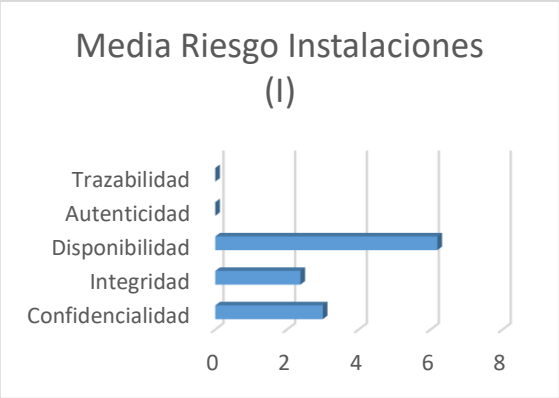

Ilustración 15: Media de riesgos en instalaciones.

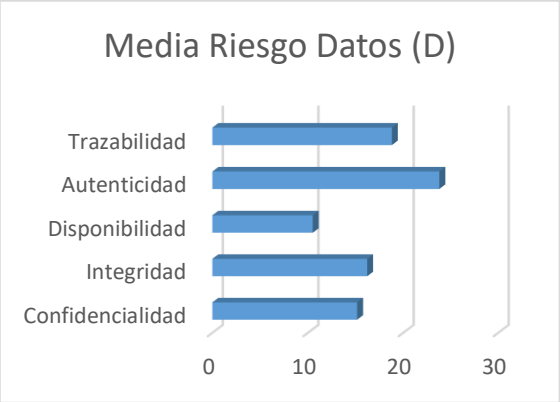

Ilustración 16: Media de riesgos en datos

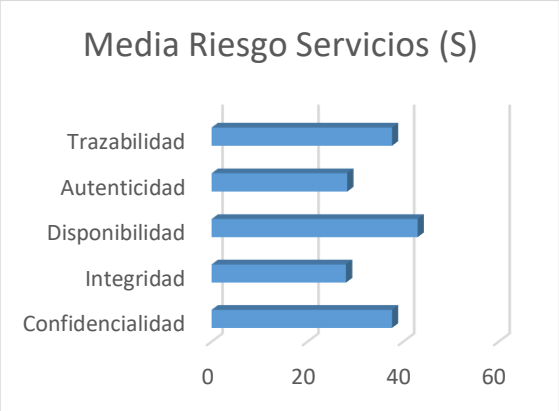

Ilustración 17: Media de riesgos en servicios.

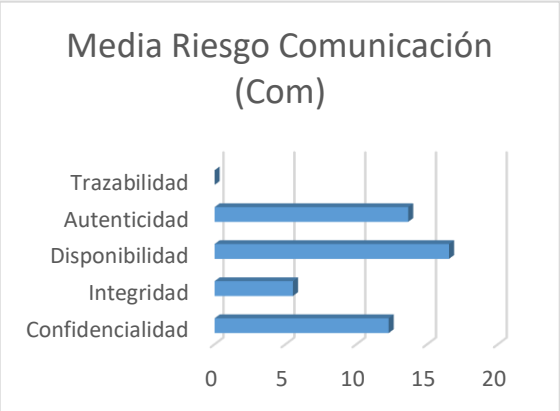

Ilustración 18: Media de riesgos en comunicación

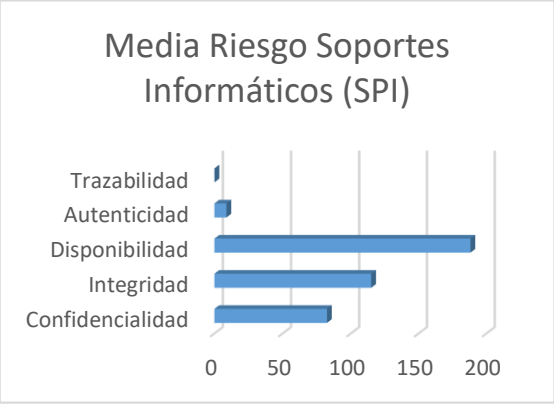

Ilustración 19: Media de riesgos soportes informáticos

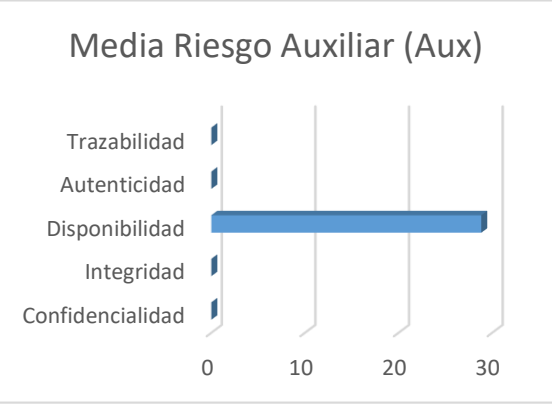

Ilustración 20: Media de riesgos elementos auxiliares

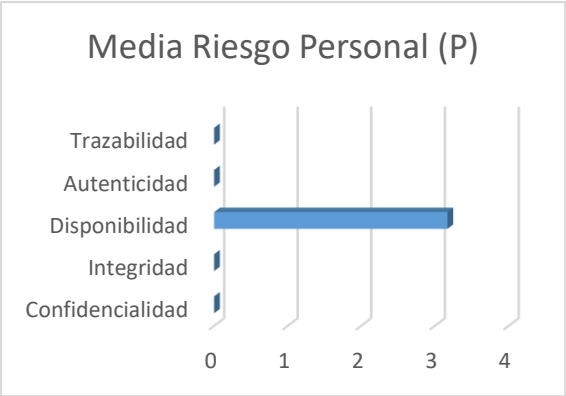

Ilustración 21 Media de riesgos en el personal.

De manera general se puede concluir que:

- El 86% de los análisis que equivale a 195 son riesgos sin mayor incidencia o nulos, el 3% que son 6 se encuentran en un estado que debe ser considerado para evitar que estos lleguen a formar parte de los riesgos en estado crítico que deben ser tratados a prioridad, los cuales al momento tienen una presencia del 12% con una equivalencia de 29 riesgos de tratamiento prioritario.
- La disponibilidad es la dependencia con mayor riesgo, tiene presencia en 45 de los 46 activos de la institución, el promedio de riesgo en este parámetro es 30.6.
- Considerando el riesgo acumulado y el valor del activo SW6 se establece que el sistema de gestión académica Prosoft Edu, la dependencia con mayor riesgo en este activo es la integridad puesto que tiende modificarse los datos sin autorización, no se descarta las otras dependencias que también están por encima del riesgo aceptable.
- La prioridad de tratamiento de riesgo se establece en el orden detallado en la siguiente tabla.

  1. SW4: Sistema académico Prosoft Edu.
  2. S1: Servicios internos, entre los cuales resaltan la conexión inalámbrica, el inventario GLPI y el servicio de monitoreo de sistemas.
  3. SPI2: Memorias USB, las cuales tienen un uso de mucha incidencia en la institución y no existen controles vitales para su funcionamiento y no propagación de software malicioso.
  4. D2: Datos Académicos, a estos se le debe dar un mejor tratamiento porque la información al momento no tiene control de custodia ni es comprobada la integridad de los datos.
  5. SW2: Windows Server 2012, este software con presencia en varios servidores internos no está licenciado, y el uso de parches expone la confidencialidad, integridad y autenticidad de los servicios alojados en estos sistemas, además de que su uso es limitado.
  6. COM1: La conexión a internet últimamente se ha visto muy perjudicada por inconvenientes propios del proveedor y en ocasiones por intentos de acceso no autorizado al router de Netlife, mismas credenciales predeterminadas que son prácticamente públicas.

7. SP1: Discos duros externos, al igual que las memorias USB son usadas para el traspaso y almacenaje de información, la diferencia con estos es que son usados por un grupo específico de la institución.
8. HW5: Laptops, estos equipos portátiles tienden a extraviarse, no existe control de permanencia o la trazabilidad de uso no es apreciable.
9. AUX1: El cableado de suministro eléctrico de la institución por la ampliación del espacio físico y aumento de instalaciones ha acogido varias modificaciones, mismas que con el paso del tiempo han denotado pronto mal funcionamiento perjudicando principalmente la disponibilidad de los servicios y a otros activos como los computadores de escritorio.
10. HW4: Computadores de escritorio, como se menciona en el punto anterior estos activos se ven mayormente afectado por los inconvenientes de energía, existen otros factores como la proliferación de virus y la mala utilización de los equipos que hacen que este tipo de hardware esté expuesto.

- Al final deben ser tratados los riesgos que se sitúan entre en 30 y 49, considerando que, de presentarse ciertas variaciones o presencia de comportamientos no habituales sobre estos, estarían propensos a superar el riesgo aceptable.

FASE 4: PROPUESTA DE PROYECTOS.

4.1 INTRODUCCIÓN.

Una vez identificados los activos vulnerables y clasificados por su uso e importancia para los procesos de la institución, es necesario plantear planes que permitan diluir al máximo los riesgos, a través de un estudio meticuloso en convergencia con otras áreas importantes de la institución como la de economato. Es importante destacar que este proyecto se plantea para tres años y contempla además del tiempo el aspecto económico y secuencia de ejecución.

Implementar un plan de seguridad es posible definirlo como la capacidad que tendrá las infraestructuras o los sistemas informáticos de la UESMA de reducir o eliminar los accidentes involuntarios o malintencionados que comprometan la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de los activos de información y los datos como tal. El proyecto se lo plantea teniendo como referencia los requerimientos ISO 27001 de la tabla 2, los controles de seguridad del Anexo A presentes en las tablas 3, 5 y 17 y el resultado de los activos en riesgo de la fase 3 en la tabla 25.

4.2 PROYECTOS PLANTEADOS A LOS DIRECTIVOS

Con los proyectos presentados en las tablas a continuación se pretende cumplir con la primera fase del ciclo de Damming (PDCA), empezando en noviembre del 2019 hasta octubre del 2022.

Nombre:	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.			
Código:	PST-001	Responsable (s):	Responsable de seguridad TIC	
Fecha inicio:	01/11/2019	Presupuesto:	$3.500 Tres mil quinientos dólares americanos.	
Fecha fin:	30/12/2019	Aprobado por:	Directivos.	
Objetivo(s):	-Establecer los lineamientos y políticas de seguridad de la información en la UESMA para salvaguardar los activos y procesos. -Dar a conocer las políticas de seguridad, el Sistema Gestor de Seguridad de la Información sus objetivos y alcance a todos los involucrados (Administrativos, Docentes, Personal de Servicios y Estudiantes/Padres de familia). -Asignar responsables de procesos asociados a la seguridad de la información y de los activos informáticos.			
Detalles:	La política de seguridad es un documento de muy alto nivel que permite demostrar el compromiso que existe frente a la seguridad de la información, en este deben constar los objetivos de seguridad, manual de procesos relacionados con lo contemplado en el alcance del SGSI y el conjunto de reglas con buenas prácticas para evitar la materialización de vulnerabilidades. Este documento debe ser de fácil acceso para todas las personas relacionadas con la institución y debe ser presentado a manera de inducción al ser aprobadas y debe existir un acuerdo firmado por todos los empleados.			
Beneficios:	1. Inminente mejora de la seguridad de activos de información y procesos relacionados con estos. 2. Continuidad de negocio 3. Responsables sobre los activos de información. 4. Mejor control de vulnerabilidades y amenazas. 5. Disminuye el riesgo en todos los activos.			
Referencia:	Requerimientos ISO 27001 - 5.2 y 6.2			
Medidor:	GIS01 IMPLEMENTACIÓN DEL SGSI – Implementación de los dominios de la ISO27002. GIS02 DIRECTIVOS INVOLUCRADOS CON LA SI			
Propuesto por:	Nombre	Cargo	Fecha	Firma
	Francisco Quiñónez	Responsable de seguridad.	23/10/2019	

Tabla 26: Proyecto Política de Seguridad de la Información.

Nombre:	PLAN DE CONTINUIDAD DE NEGOCIO - PCN			
Código:	PST-002	Responsable (s):	Comité de seguridad	
Fecha inicio:	01/01/2020	Presupuesto:	$1.200,00 Mil doscientos dólares americanos	
Fecha fin:	31/03/2020	Aprobado por:	Directivos.	
Objetivos:	Desarrollar un plan que permita a la institución continuar con sus procesos frente a la ocurrencia de cualquier acontecimiento adverso con el mínimo coste posible.			
Detalles:	Conociendo los resultados del análisis de riesgo es posible conocer cuáles son los activos y procesos que pueden verse perjudicados por la consecución de cualquier amenaza, es por ello que se realiza el presente PCN, mismo que debe ser actualizado anualmente basado en las auditorios internas y cada tres años por la auditoria externa.			
Beneficios:	1. Garantizar que la institución siga sus procesos en caso de desastres. 2. Todo el personal capacitado y preparado para actuar en caso de. 3. Evitar pérdidas económicas por inactividad de activos. 4. Mínimo de inversión necesaria para el cumplimiento del PCN. 5. Disminuye el riesgo en los activos SW6, S1, D2, SW2, COM1, AUX1			
Referencia:	Controles de seguridad ISO27001 – 17.1			
Medidor:	Existencia del plan de continuidad de negocio.			
Propuesto por:	Nombre	Cargo	Fecha	Firma
	Francisco Quiñonez	Responsable de seguridad	23/10/2019	

Tabla 27: Plan de continuidad de negocios

Nombre:	FORMACIÓN Y CONCIENTIZACIÓN DE EMPLEADOS			
Código:	PST-003	Responsable (s):	Gestión de Talento Humano	
Fecha inicio:	01/04/2020	Presupuesto:	NO APLICA.	
Fecha fin:	28/05/2020	Aprobado por:	Comité de seguridad de la información.	
Objetivos:	Disponer de personal capacitado e involucrado con procesos que permitan mitigar el riesgo de los activos de información.			
Detalles:	Elaborar una planificación que permita capacitar a todo el personal de la UESMA con temas relacionados a la seguridad de la información, dando prioridad a quienes por su rol se relacionan directamente con los activos, pero al final todos dispongan de buenas prácticas y manejo correcto de las TICS. Los empleados que cesen sus funciones sabrán cuál es su responsabilidad referente a los sistemas de información de la institución aun estando fuera de la UESMA, respaldados en el contrato de trabajo que debe incluir cláusulas relacionadas a lo expuesto			
Beneficios:	1. Los activos y procesos estarán más seguros. 2. Menos costes en reposición de activos. 3. Mayor disponibilidad de activos y sistemas de información. 4. Disminuye el riesgo en los activos SPI1, SPI2, HW4, HW5			
Referencia:	Controles de seguridad A7.1 A7.2 A7.3			
Medidor:	GIS05 – INDUCCIÓN AL PERSONAL			
Propuesto por:	Nombre	Cargo	Fecha	Firma
	Francisco Quiñónez	Responsable de Seguridad	06/11/2019	

Tabla 28: Proyecto Formación y concientización de empleados.

Nombre:	TRATAMIENTO DE LA INFORMACIÓN DE GTH.			
Código:	PST-004	Responsable (s):	Jefe GTH	
Fecha inicio:	10/06/2020	Presupuesto:	$ 3.400,00 Tres mil cuatrocientos dólares americanos.	
Fecha fin:	30/06/2020	Aprobado por:	Comité de seguridad de la información.	
Objetivos:	Proteger la toda la información referente a los empleados de la institución.			
Detalles:	Diseñar mecanismos e implementar estructura físicas y lógicas (software) que permitan asegurar el cuidado, no divulgación y deterioro de la información de todos los empleados y exempleados de la UESMA, asignando roles y responsabilidades desde el momento de ingreso a la institución.			
Beneficios:	1. Roles y responsabilidades bien definidas. 2. Procedimientos bien estructurados en el departamento de GTH. 3. Definición de procesos disciplinarios en todos los escenarios para los trabajadores. 4. Cumplimiento legislativo relacionado al cuidado y responsabilidad de datos de las personas. 5. Disminuye el riesgo en los activos D2, S1			
Referencia:	Controles de seguridad de la información A18.1			
Indicador:	GIS6 – SEGURIDAD FÍSICA Y AMBIENTAL. GIS10 – ANÁLISIS DE VULNERABILIDADES.			
Propuesto por:	Nombre	Cargo	Fecha	Firma
	Francisco Quiñonez	Responsable de seguridad.	15/11/2019	

Tabla 29: Proyecto Tratamiento de la información de GTH.

Nombre:	CLASIFICACIÓN DE LA INFORMACIÓN.			
Código:	PST-005	Responsable (s):	Comité de seguridad de información.	
Fecha inicio:	02/07/2020	Presupuesto:	$ 2.000,00 Dos mil dólares americanos.	
Fecha fin:	29/07/2020	Aprobado por:	Comité de seguridad de la información.	
Objetivos:	Asegurar, clasificar, etiquetar y establecer procesos de manipulación de la información, basados en la fuente generadora.			
Detalles:	Existen muchos sistemas, activos, procesos y otros elementos que generan información en la institución, estas fuentes pueden ser de lo más variada sin importar de donde provenga puede tener una variedad de valores e importancia y así mismo controles que permitan salvaguardarla.			
Beneficios:	1. Identificación rigurosa del tipo de información existente en la UESMA, según su valor económico, criticidad, dependencia legales y caracterización. 2. Seguridad de la información bien definida por niveles. 3. Procesos y responsables definidos en la manipulación de la información. 4. Disminuye el riesgo en los activos S1, D2			
Referencia:	Requerimiento ISO 27001 A8.2			
Indicador:	Verificación de cumplimiento anual.			
Propuesto por:	Nombre	Cargo	Fecha	Firma
	Francisco Quiñonez	Responsable de seguridad.	15/11/2019	

Tabla 30: Proyecto Clasificación de la información.

Nombre:	SISTEMAS DE GESTIÓN DE USUARIOS			
Código:	PST-006	Responsable (s):	Departamento TIC	
Fecha inicio:	01/08/2020	Presupuesto:	$ 3.750,00 Tres mil setecientos cincuenta dólares americanos.	
Fecha fin:	31/10/2020	Aprobado por:	Comité de seguridad de la información	
Objetivos:	-Gestionar de manera correcta los roles y permisos asignados a los usuarios según el nivel y las funciones que cumplen. -Constatar de forma clara y transparente de la trazabilidad de uso de los activos/sistemas de información.			
Detalles:	Los activos y sistemas de información de la institución deben poseer un método que permita controlar el acceso al mismo, identificar los usuarios y tiempo de uso, impedir el acceso no autorizado, quitar/otorgar permisos y accesos y controlar el uso.			
Beneficios:	1. Mayor control de seguridad en acceso a los activos y sistemas de información. 2. Evitar tiempo de ocio en horas laborables. 3. Evitar perdida o divulgación de información sensible. 4. Disminuye el riesgo en los activos SW6, D2, SW2, HW4, HW5			
Referencia:	Requisitos ISO 27001 A9.2 A9.4			
Indicador:	GIS04 USO DE ACTIVOS. GIS07 CONTROL DE ACCESO.			
Propuesto por:	Nombre	Cargo	Fecha	Firma
	Francisco Quiñonez	Responsable de seguridad.	15/11/2019	

Tabla 31: Proyecto Sistemas de gestión de usuarios.

Nombre:	GESTIÓN DE INCIDENTES			
Código:	PST-007	Responsable (s):	Responsable de seguridad de la información	
Fecha inicio:	1/11/2020	Presupuesto:	No aplica.	
Fecha fin:	30/10/2022	Aprobado por:	Comité de seguridad de la información.	
Objetivos:	-Identificar a tiempo y registrar los incidentes en la seguridad de la información.			
Detalles:	Es necesario que aquellos inconvenientes que se presentan en la seguridad de la información sean identificados de manera óptima con el fin de activar los lineamientos planteados en el PCN, estos incidentes deben ser registrados y documentados con el fin de aprender de ellos y así evitar futuras instigaciones del mismo tipo.			
Beneficios:	1. Procesos definidos para la gestión de incidentes. 2. Responsabilidades definidas en la gestión de incidentes. 3. Registro de evidencias de lo ocurrido. 4. Aprendizaje basado en las incidencias. 5. Control de incidentes y optimización de tiempo de respuesta. 6. Disminuye el riesgo en los activos SW6, S1, D2, SW2, HW4, HW5			
Referencia:	Requerimiento ISO 27001 A16.1			
Indicador:	Incidentes de seguridad documentados con una periodicidad de 6 meses. GIS03 INCIDENTES DE SEGURIDAD.			
Propuesto por:	Nombre	Cargo	Fecha	Firma
	Francisco Quiñonez	Responsable de seguridad.	15/11/2019	

Tabla 32: Proyecto Gestión de incidentes.

Nombre:	USO DE DISPOSITIVOS MÓVILES Y PORTATILES			
Código:	PST-008	Responsable (s):	Responsable de seguridad de la información.	
Fecha inicio:	01/01/2021	Presupuesto:	No aplica	
Fecha fin:	30/06/2021	Aprobado por:	Comité de seguridad de la información.	
Objetivos:	Concientizar a los empleados sobre el uso adecuado de los dispositivos. Evitar la propagación de software malicioso dentro de la institución. Controlar la existencia y usabilidad de los dispositivos.			
Detalles:	En la institución se pone a disposición de docentes y administrativos dispositivos de almacenamiento extraíble y computadoras portátiles, mismas que deben ser usadas de manera correcta basada en lineamientos planteados en este proyecto, así mismo es necesario realizar la constatación física de existencia y uso de los mismos			
Beneficios:	1. Disponibilidad de los dispositivos móviles y portátiles para procesos necesarios. 2. Control de uso de dispositivos. 3. Mitigar el riesgo de propagación de software malicioso. 4. Disminuye el riesgo en los activos SPI1, SPI2, HW5			
Referencia:	Requerimiento ISO 27001 A6.2.1 A8.3			
Indicador:	GIS04 USO DE ACTIVOS. GIS09 PROTECCION CONTRA SOFTWARE MALICIOSO. Verificación de uso mensual.			
Propuesto por:	Nombre	Cargo	Fecha	Firma
	Francisco Quiñonez	Responsable de seguridad.	15/11/2019	

Tabla 33: Proyecto Uso de dispositivos móviles y portátiles

Nombre:	MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.			
Código:	PST-009	Responsable (s):	Departamento TI.	
Fecha inicio:	02/03/2021	Presupuesto:	$7.650,00 Siete mil seiscientos cincuenta dólares americanos.	
Fecha fin:	10/06/2021	Aprobado por:	Directivos	
Objetivos:	Garantizar la disponibilidad de los activos y sistemas de información.			
Detalles:	Planificar el proceso de mantenimiento y actualización, en caso de ser necesario, de los activos y sistemas de información involucrados en el SGSI, con el fin de prever cualquier irregularidad existente y garantizar la funcionabilidad ininterrumpida de estos. Parchar los sistemas de información también forma parte de este proyecto así como licenciar los que sean necesarios.			
Beneficios:	1. Continuidad de negocio. 2. Mitigación de riesgos. 3. Evitar pérdidas económicas en caso de alguna perturbación de los activos. 4. Disminuye el riesgo en los activos SW6, S1, D2, SW2			
Referencia:	Requerimiento ISO 27001 A14			
Indicador:	Registro de incidencias en los sistemas de información. Documentación de constatación de este proceso anualmente.			
Propuesto por:	Nombre	Cargo	Fecha	Firma
	Francisco Quiñonez	Responsable de seguridad.	15/11/2019	

Tabla 34: Proyecto Mantenimiento de los sistemas de información.

Nombre:	MONITOREO DE RED			
Código:	PST-010	Responsable (s):	Responsable de seguridad de la información.	
Fecha inicio:	01/11/2020	Presupuesto:	No aplica.	
Fecha fin:	31/10/2022	Aprobado por:	Comité de seguridad de la información.	
Objetivos:	Mejorar la disponibilidad y calidad de los servicios internos de la institución y la conexión hacia internet y los servicios externos.			
Detalles:	A través del software ya disponible en la institución Endian Firewall monitorizar de manera permanente el consumo de la red y uso de internet de todos los usuarios conectados con el fin de priorizar la disponibilidad para aquellos procesos y activos que mayor representatividad tienen para los procesos críticos de la institución.			
Beneficios:	1. Eficiencia en procesos relevantes para la UESMA que hacen uso de los recursos de red. 2. Detectar conexiones de red anormales. 3. Identificar usuarios que no den uso adecuado a la red. 4. Optimizar el consumo de la red. 5. Detectar ataques. 6. Disminuye el riesgo en los activos SW6, S1, D2, SW2, COM1			
Referencia:	Requerimiento ISO27001 A13.1			
Indicador:	GIS10 ANÁLISIS DE VULNERABILIDADES. Resultados del monitoreo de red mensual.			
Propuesto por:	Nombre	Cargo	Fecha	Firma
	Francisco Quiñonez	Responsable de seguridad.	15/11/2019	

Tabla 35: Proyecto Monitoreo de red.

Nombre:	GESTIÓN DE ACTIVOS			
Código:	PST-011	Responsable (s):	Jefe de bodega	
Fecha inicio:	15/07/2021	Presupuesto:	$ 1.900,00 Mil novecientos dólares americanos.	
Fecha fin:	30/10/2021	Aprobado por:	Comité de seguridad de la información.	
Objetivos:	Clasificar, asegurar, garantizar y verificar la permanencia de los activos de información.			
Detalles:	El hardware es el tipo de activos con mayor representatividad en el levantamiento de los activos de información contemplados en el SGSI por lo tanto es necesario se implementen procesos y sistemas que permitan garantizar la disponibilidad y permanencia de estos.			
Beneficios:	1. Evitar uso de recursos económicos en reposición de activos. 2. Trazabilidad de uso de los activos y sistemas de información. 3. Garantizar la disponibilidad de los activos de información. 4. Disminuye el riesgo en los activos SPI1, SPI2, HW4, HW5			
Referencia:	Requerimientos ISO27001 A8.1			
Indicador:	GIS04 USO DE ACTIVOS. Documentación que respalde el proceso realizado de manera mensual.			
Propuesto por:	Nombre	Cargo	Fecha	Firma
	Francisco Quiñonez	Responsable de seguridad.	30/10/2019	

Tabla 36: Proyecto Gestión de activos.

Nombre:	REDES DE DATOS Y COMUNICACIÓN			
Código:	PST-012	Responsable (s):	Responsable de seguridad de la información.	
Fecha inicio:	02/02/2020	Presupuesto:	$ 8.750,00 Dos mil setecientos cincuenta dólares americanos.	
Fecha fin:	30/05/2020	Aprobado por:	Comité de seguridad de la información.	
Objetivos:	Optimizar el uso y consumo de la red de datos para garantizar la disponibilidad de las mismas y la calidad de servicios en las comunicaciones.			
Detalles:	Existe un sustancial crecimiento en la infraestructura informática de la UESMA desde que fue entregado el proyecto implementación de la red, por lo cual es necesario realizar actualizaciones lógicas en los sistemas de información y comunicación para optimizar los recursos de red.			
Beneficios:	1. Optimización de procesos primordiales para la institución. 2. Planificación de escalabilidad. 3. Optimización de recursos lógicos y económicos. 4. Establecer políticas de uso de red. 5. Disminuye el riesgo en los activos SW6, S1, D2, SW2, COM1			
Referencia:	Requisitos ISO27001 A9.1 A13.1			
Indicador:	GIS04 USO DE ACTIVOS Verificación de optimización en procesos relacionados a las redes de datos y comunicación de manera mensual.			
Propuesto por:	Nombre	Cargo	Fecha	Firma
	Francisco Quiñonez	Responsable de seguridad.	20/11/2019	

Tabla 37: Proyecto Redes de datos y comunicación.

Nombre:	COPIAS DE SEGURIDAD			
Código:	PST-013	Responsable (s):	Responsable de seguridad de la información.	
Fecha inicio:	02/01/2021	Presupuesto:	$ 2.180,00 Dos mil ciento ochenta dólares americanos.	
Fecha fin:	01/06/2021	Aprobado por:	Directivos	
Objetivos:	Definir políticas y mecanismos que permitan automatizar la ejecución de copias de seguridad en los sistemas de información para garantizar la integridad y disponibilidad de los datos.			
Detalles:	Frente a todos los controles establecidos existe posibilidad de materialización de amenazas que pueden ocasionar perdida de información, es por ello que esta debe respaldarse de tal manera que el acceso a estos respaldos sea en los niveles de seguridad AAAA.			
Beneficios:	1. Redundancia de datos. 2. Disponibilidad de la información. 3. Evitar pérdidas económicas por perdida de información del mismo carácter. 4. Disminuye el riesgo en los activos SW6, D2, SW2			
Referencia:	Requisitos ISO27001 A12.3			
Indicador:	GIS08 BACKUPS			
Propuesto por:	Nombre	Cargo	Fecha	Firma
	Francisco Quiñonez	Responsable de seguridad.	20/11/2019	

Tabla 38: Proyecto Copias de seguridad

Nombre:	SEGURIDAD FÍSICA, AMBIENTAL Y LÓGICA			
Código:	PST-014	Responsable (s):	Responsable de seguridad de la información.	
Fecha inicio:	02/08/2022	Presupuesto:	$ 4.300,00 Cuatro mil trescientos dólares americanos.	
Fecha fin:	01/10/2022	Aprobado por:	Directivos	
Objetivos:	Garantizar la seguridad de los activos y sistemas de información frente a riesgos de acceso físico, lógico y las exposiciones frente a desastres ambientales.			
Detalles:	Existen activos que están expuestos a acceso de cualquier persona que tenga acceso a la institución, pero por su carácter crítico de la información que contienen deben tener una lista muy limitada de usuarios que pueden tener acceso a los mismos y esto debe ser controlado. El medio es propenso a desastres naturales tales como inundaciones que se han presentado anualmente en épocas de lluvias y movimientos telúricos con una frecuencia mensual en el último año. Es por ello que se deben tomar las medidas necesarias para evitar que en la ocurrencia de este tipo de desastres o accesos mal intencionados se vean perjudicados los activos			
Beneficios:	1. Autenticidad de la información. 2. Garantizar disponibilidad de los activos según uso y perfiles. 3. Evitar gastos en reposición de activos o restauración de los mismos. 4. Aporte para el plan de continuidad de negocio. 5. Disminuye el riesgo en los activos HW4, HW5, AUX1			
Referencia:	Requisitos ISO27001 A11.2			
Indicador:	GIS03 INCIDENTES DE SEGURIDAD.			
Propuesto por:	Nombre	Cargo	Fecha	Firma
	Francisco Quiñonez	Responsable de seguridad.	20/11/2019	

Tabla 39: Proyecto Seguridad física, ambiental y lógica.

Nombre:	AUDITORIAS			
Código:	PST-015	Responsable (s):	Responsable de seguridad de la información.	
Fecha inicio:	30/11/2019	Presupuesto:	No aplica.	
Fecha fin:	30/11/2022	Aprobado por:	Directivos	
Objetivos:	Comprobar la efectividad de los proyectos y planes de mejoras planteados verificando el cumplimiento de los mismos de acuerdo a lo planificado.			
Detalles:	A medida que se ejecuten los proyectos anteriormente descritos debe existir un proceso, interno en primera instancia, que compruebe que las medidas tomadas para mitigar el riesgo presentado en los activos o sistemas de información, o incluso en la documentación de los procesos relacionados con el SGSI.			
Beneficios:	1. Mejora de procesos de auditoria. 2. Evitar uso de recursos económicos en proyectos que no generan beneficio para la institución. 3. Mejora y actualización de proyectos planteados y el SGSI. 4. Disminuye el riesgo en todos los activos			
Referencia:	Requisitos ISO27001 A18.2			
Indicador:	Resultados de auditorías y planes de mejoras propuestos			
Propuesto por:	Nombre	Cargo	Fecha	Firma
	Francisco Quiñonez	Responsable de seguridad.	20/11/2019	

Tabla 40: Proyecto Auditorias

5.3 RESUMEN ECONÓMICO

Código	Fecha Inicio	Fecha Fin	Presupuesto	Justificación
PST-001	1/11/2019	30/12/2019	$ 3,500.00	Legalización y respaldos reglamentarios de las políticas.
PST-002	1/1/2020	31/3/2020	$ 1,200.00	Comisión por servicios adicionales
PST-003	6/2/2020	5/3/2020	N/A	
PST-004	10/3/2020	31/3/2020	$ 3,400.00	Inmuebles y desarrollo de app y bdd
PST-005	2/4/2020	29/4/2020	$ 2,000.00	Comisión por servicios adicionales
PST-006	1/5/2020	31/7/2020	$ 3,750.00	Licencias de Windows server para uso de Directorio Activo.
PST-007	1/11/2020	30/10/2022	N/A	
PST-008	1/1/2021	30/6/2021	N/A	
PST-009	2/3/2021	10/6/2021	$ 7,650.00	Insumos de limpieza, adquisición de software actualizado y reposición de elementos.
PST-010	1/11/2020	31/10/2022	N/A	
PST-011	15/7/2021	30/10/2021	$ 1,900.00	Insumos de etiquetado y lector de barras.

PST-012	2/2/2020	30/5/2020	$ 8,750.00	Adquisición de equipos de comunicación, adecuaciones en la infraestructura física, comisiones por servicios adicionales.
PST-013	2/1/2021	1/6/2021	$ 2,180.00	Adquisición de sistema de gestión de copias de seguridad.
PST-014	2/8/2022	1/10/2022	$ 4,360.00	Adecuaciones en infraestructura física y comisión por servicios adicionales
PST-015	30/11/2019	30/11/2022	N/A	
TOTAL			**$ 38,690.00**	

Al finalizar la fase **Check** del primer ciclo PDCA, se prevé solucionar las incidencias detectadas identificadas dentro del Sistema de Gestión de Seguridad de la Información y posterior a esto se procede a la fase **Act** finalizada la auditoria interna, la cual emitirá los resultados de cumplimiento de los requisitos que establece la norma ISO 27001, y así se puede constatar el producto de los proyectos y controles realizados.

La siguiente tabla presenta un diagrama de gantt con la planificación de los proyectos anteriormente propuestos en los tres años que dura el sistema gestor de la seguridad de la información,

PROY.	2019		2020												2021												2022									
Código	Noviembre	Diciembre	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre
PST-001																																				
PST-002																																				
PST-003																																				
PST-004																																				
PST-005																																				
PST-006																																				
PST-007																																				
PST-008																																				
PST-009																																				
PST-010																																				
PST-011																																				
PST-012																																				
PST-013																																				
PST-014																																				
PST-015																																				

Tabla 41: Diagrama de Gantt, proyectos de mejora.

4.4 MODIFICACIÓN DEL RIESGO

En contraste con el análisis realizado en la fase 3, es necesario realizar una nueva tabla que permita apreciar la valoración de riesgos en los activos luego de aplicar los proyectos y mejoras, mismos que se encuentran focalizados en aquellos activos que superan el riesgo aceptable >50 y aquellos que estaban próximos a superar el riesgo aceptable >40 y <49, pero estos proyectos también beneficien a activos que no estaban en riesgo. En la tabla 41 se puede constatar que los activos que estaban en riesgos o próximos a alcanzar el nivel, presentan una gran variación en beneficio de la seguridad de la información.

TIPO	ID_ACTIVO	FRECUENCIA		% I POTENCIAL					RIESGO				
		Num.	Cual.	C	I	D	A	T	C	I	D	A	T
HW	HW1	0.01	FMB	10	4.5	10	0	0	0.1	0.045	0.1	0	0
	HW2	0.01	FMB	9	4.5	7	0	0	0.09	0.045	0.07	0	0
	HW3	0.01	FMB	4	2.3	8	0	0	0.04	0.0225	0.08	0	0
	HW4	1	FM	3.8	1.5	5.3	0	0	3.75	1.5	5.25	0	0
	HW5	1	FM	5.3	1.3	4.5	0	3.5	5.25	1.25	4.5	0	3.5
	HW6	0.01	FMB	0.8	0.8	2.5	0	0	0.0075	0.0075	0.025	0	0
	HW7	0.01	FMB	1.5	0.5	3	0	0	0.015	0.005	0.03	0	0
	HW8	0.01	FMB	5.3	6	3.8	0	2.5	0.0525	0.06	0.0375	0	0.025
	HW9	0.1	FB	1.5	3.8	1.5	0	5.3	0.15	0.375	0.15	0	0.525
	HW10	0.01	FMB	0.1	0.1	0.8	0	0	0.0005	0.001	0.0075	0	0
SW	SW1	0.1	FB	6	6	8	0	0	0.6	0.6	0.8	0	0
	SW2	1	FM	8	9	6.8	6.8	0	8	9	6.75	6.75	0
	SW3	0.1	FB	3	4	2.5	3	0	0.3	0.4	0.25	0.3	0
	SW4	0.1	FB	3	3	3.8	3	0	0.3	0.3	0.375	0.3	0
	SW5	0.1	FB	0.3	1	1	0	1	0.025	0.1	0.1	0	0.1
	SW6	1	FM	7	10	9	9	6	7	10	9	9	6
I	I1	1	FM	5	4.5	10	0	0	5	4.5	10	0	0
	I2	0.1	FB	3.5	4	8	0	0	0.35	0.4	0.8	0	0
	I3	1	FM	0.5	1	4.5	0	0	0.5	1	4.5	0	0
	I4	1	FM	3	0	2.3	0	0	3	0	2.25	0	0
D	D1	0.1	FB	10	7.5	4	10	8	1	0.75	0.4	1	0.8
	D2	1	FM	5.3	6	4	9	7	5.25	6	4	9	7
	D3	0.1	FB	8	7.5	4.5	10	9	0.8	0.75	0.45	1	0.9
	D4	0.1	FB	5.3	6	4	9	7	0.525	0.6	0.4	0.9	0.7
	D5	0.1	FB	5.3	6	4	9	7	0.525	0.6	0.4	0.9	0.7
COM	COM1	0.1	FB	5.3	2	7	6	0	0.525	0.2	0.7	0.6	0

	COM2	0.01	FMB	5.3	6	7	3.8	0	0.0525	0.06	0.07	0.0375	0
	COM3	0.01	FMB	1	0.3	5.3	4	0	0.01	0.0025	0.0525	0.04	0
	COM4	0.1	FB	3	1	4.5	3.8	0	0.3	0.1	0.45	0.375	0
	COM5	0.01	FMB	5.3	6	7	3.8	0	0.0525	0.06	0.07	0.0375	0
S	S1	0.1	FB	7	5.3	8	5.3	7	0.7	0.525	0.8	0.525	0.7
	S2	0.1	FB	5.3	3.5	6	4	5.3	0.525	0.35	0.6	0.4	0.525
SPI	SPI1	0.1	FB	3	6	5.3	3.5	0	0.3	0.6	0.525	0.35	0
	SPI2	1	FM	3	4	7	0	0	3	4	7	0	0
	SPI3	0.01	FMB	0	0	4.5	0	1.5	0	0	0.045	0	0.015
	SPI4	0.01	FMB	0	0	2.5	0	1.5	0	0	0.025	0	0.015
AUX	AUX1	0.1	FB	0	0	10	0	0	0	0	1	0	0
	AUX2	0.1	FB	0	0	10	0	0	0	0	1	0	0
	AUX3	0.01	FMB	0	0	0.8	0	0	0	0	0.0075	0	0
	AUX4	0.01	FMB	0	0	5.3	0	0	0	0	0.0525	0	0
P	P1	0.1	FB	0	0	4.5	0	0	0	0	0.45	0	0
	P2	0.1	FB	0	0	3.8	0	0	0	0	0.375	0	0
	P3	0.1	FB	0	0	2	0	0	0	0	0.2	0	0
	P4	1	FM	0	0	3	0	0	0	0	3	0	0
	P5	10	FA	0	0	1	0	0	0	0	10	0	0
	P6	10	FA	0	0	0.5	0	0	0	0	5	0	0

Tabla 42: Riesgo de activos posterior a aplicación de proyectos de mejora.

En cuanto a los controles del Anexo A y los requerimientos de la ISO 27001 se presentan importantes modificaciones en incongruencia con el análisis referencial realizado en la fase 2 del SGSI, a continuación, se presenta la tabla de resultados posterior a la aplicación de los proyectos.

Estado	Significado	Proporción de requerimientos SGSI	Proporción de Controles de Seguridad de la Información
? Desconocido	No ha sido verificado	**0%**	**0%**
Inexistente	No se lleva a cabo el control de seguridad en los sistemas de información.	**0%**	**0%**
Inicial	Las salvaguardas existen, pero no se gestionan, no existe un proceso formal para realizarlas. Su éxito depende de la buena suerte y de tener personal de la alta calidad.	**0%**	**0%**

Repetible	La medida de seguridad se realiza de un modo totalmente informal (con procedimientos propios, informales). La responsabilidad es individual. No hay formación.	**0%**	**0%**
Definido	El control se aplica conforme a un procedimiento documentado, pero no ha sido aprobado ni por el Responsable de Seguridad ni el Comité de Dirección.	**15%**	**16%**
Administrado	El control se lleva a cabo de acuerdo a un procedimiento documentado, aprobado y formalizado.	**37%**	**61%**
Optimizado	El control se aplica de acuerdo a un procedimiento documentado, aprobado y formalizado, y su eficacia se mide periódicamente mediante indicadores.	**48%**	**16%**
No aplicable	A fin de certificar un SGSI, todos los requerimientos principales de ISO/IEC 27001 son obligatorios. De otro modo, pueden ser ignorados por la Administración.	**0%**	**7%**

Tabla 43: Resultado de controles Anexo A y requisitos ISO27001

Finalmente se presenta el gráfico GAP propuesto por la ISO 27002 posterior a los proyectos de seguridad planteados.

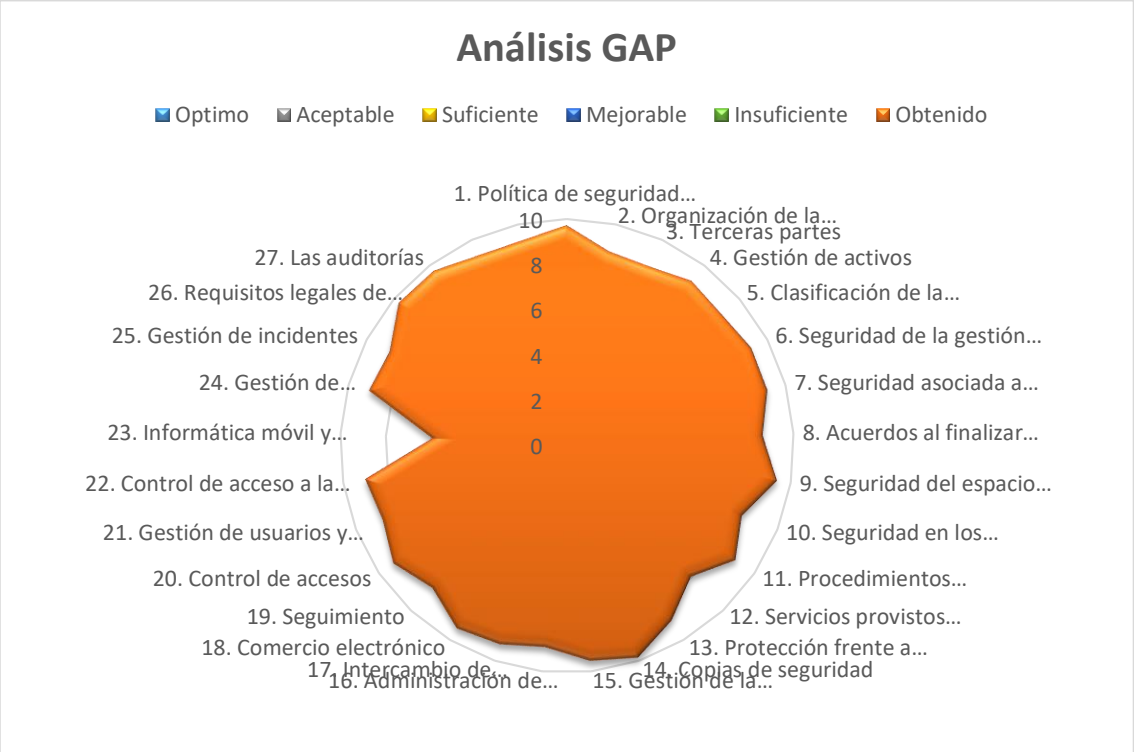

Ilustración 22: Análisis GAP resultado.

4.5 CONCLUSIONES

Al finalizar esta fase y poder realizar la asimilación entre los resultados de la fase 2 de análisis referencial y la fase 3 de análisis de riesgos contra lo apreciado en esta la etapa 4 que contempla los proyectos que pretenden mejorar la seguridad de la información en la UESMA, es apreciable que los resultados esperados al inicio de la implementación del SGSI se han cumplido a cabalidad, brindando un muy buen nivel respecto a la SI en la institución, no solo en mejorando la seguridad de los activos en riesgo si no también los que están por debajo del mínimo aceptable, no obstante, es importante acentuar que la informática es una rama que tiene actualización constante y por lo tanto las amenazas y vulnerabilidades de igual manera, es por ello que es necesario realizar revisiones periódicas de los resultados que emitan las auditorías internas para estar siempre a la vanguardia de las nuevas tendencias de la seguridad de la información.

FASE 5: AUDITORIA

5.1 INTRODUCCIÓN

Una auditoria es el proceso por el cual se realiza un examen crítico y sistemático para realizar una investigación de los objetivos, planes y procesos, estudiar las políticas establecidas y el cumplimiento de las mismas, analizar la eficiencia de la utilización de los activos y el personal, manejo de la información entre otros aspectos enmarcados en el sistema gestor de la seguridad de la información, la persona o el grupo de personas responsables de ejecutar las auditorías internas deben ser quienes tengan domino de la seguridad de la información, para el caso particular de la UESMA, el responsable de la seguridad de la información.

5.2 METODOLOGÍA

Para el proceso de auditoria se utiliza el Modelo de Madurez de Capacidades (CMM) que evaluará los 14 dominios y los 114 controles contemplados en la ISO/IEC 27002:2013, mismos controles del Anexo A, esto permitirá conocer el nivel de madurez de la seguridad de la información contemplada en el Sistema Gestor de Seguridad de la Información, los dominios a evaluar son:

- ✓ Política de seguridad de la información.

- ✓ Organización de la seguridad de la información
- ✓ Gestión de activos.
- ✓ Clasificación de la información.
- ✓ Seguridad de la gestión de recursos humanos.
- ✓ Seguridad asociada a funciones
- ✓ Acuerdos al finalizar contratos.
- ✓ Seguridad del espacio físico.
- ✓ Seguridad en los activos informáticos.
- ✓ Procedimientos operativos y responsabilidades.
- ✓ Cumplimiento.

En cuanto a los requisitos que establece la ISO 27001 para la seguridad de la información y en exclusiva del Sistema Gestor de Seguridad de la Información también serán presentados los resultados con la tabla CMM. Los requisitos generales a presentar son:

- ✓ Contexto de la organización.
- ✓ Liderazgo.
- ✓ Planificación.
- ✓ Soporte.
- ✓ Operación.
- ✓ Evaluación del desempeño.
- ✓ Mejora.

El análisis de estos controles y requisitos se realiza de acuerdo a la tabla 44 que contiene los posibles estados de acuerdo a la madurez, estos se muestran en la tabla continuación.

EFECTIVIDAD	CMM	SIGINIFICADO	DESCRIPCIÓN
0-10%	L0	Inexistente	Carencia completa de cualquier proceso reconocible
10-50%	L1	Inicial / Ad-hoc	Estado inicial donde el éxito de las actividades de los procesos se basa la mayoría de las veces en el esfuerzo personal, estos procesos son generalmente localizados en áreas concretas

50-70%	L2	Reproducible / Intuitivo	Procesos similares se llevan en forma parecida por diferentes responsables de la misma tarea, se aprenden de las buenas experiencias y se tratan de replicar, no existen bases ni formación para la ejecución de procesos.
70-80%	L3	Definido	La institución conoce y participa del proceso, estos procesos están implantados, documentados, aprobados y comunicados. Todos en la organización forman parte de la preparación.
80-90%	L4	Gestionado / Medible	Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos. Se dispone de tecnología para automatizar el flujo de trabajo, se tienen herramientas para mejorar la calidad y la eficiencia.
90-100%	L5	Optimizado	Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos

Tabla 44: Análisis de madurez CMM

5.3 RESULTADOS

A continuación, se presentan un resumen de los resultados obtenidos de lo expuesto en la metodología de este apartado, luego de analizar los 114 controles del Anexo A y los 27 requisitos que establece la ISO 27001 y a cada uno establecerle un nivel de acuerdo a los presentados en la tabla de análisis de madurez CMM. Para revisar el detalle del análisis ir al anexo I y anexo II

N°	Sección	Dominio SI	ACTUAL		INCIAL	
			CMM	%	CMM	%
1	A5	Política de seguridad de la información.	L4	81.00%	L0	3.00%
2	A6	Organización de la seguridad de la información.	L3	79.70%	L1	11.80%

3	A7	Seguridad relativa a los recursos humanos.	L5	90.22%	L0	6.17%
4	A8	Gestión de activos.	L3	71.03%	L1	37.67%
5	A9	Control de acceso.	L3	75.19%	L1	12.18%
6	A10	Criptografía	L2	63.50%	L0	4.50%
7	A11	Seguridad física y del entorno.	L5	92.72%	L2	64.19%
8	A12	Seguridad de las operaciones.	L4	86.85%	L2	59.39%
9	A13	Seguridad de las comunicaciones.	L4	85.83%	L1	35.46%
10	A14	Adquisición, desarrollo y mantenimiento de los sistemas de información.	L4	83.72%	L2	63.56%
11	A15	Relación con proveedores	L3	78.58%	L2	65.50%
12	A16	Gestión de incidentes de seguridad de la información.	L4	84.57%	L2	52.29%
13	A17	Aspectos de seguridad de la información para la gestión de la continuidad de negocio	L4	82.50%	L2	55.33%
14	A18	Cumplimiento	L4	82.50%	L1	18.50%
		Requerimiento ISO 27001				
15	4	Contexto de la organización	L3	79.88%	L0	9.50%
16	5	Liderazgo	L3	76.67%	L1	30.67%
17	6	Planificación	L4	83.50%	L1	19.17%
18	7	Soporte	L3	74.47%	L1	13.80%
19	8	Operación	L4	82.33%	L1	25.00%
20	9	Evaluación del desempeño	L3	75.67%	L0	0.00%
21	10	Mejora	L4	81.50%	L1	42.50%

Tabla 45: Auditoria en Anexo A y requerimientos ISO27001

De acuerdo a los controles que establece la ISO 27002 para el análisis de cumplimiento, de acuerdo al estado del modelo de madurez de capacidades se obtiene la ilustración 23 que muestra la cantidad de controles por cada nivel y la ilustración 24 los requisitos.

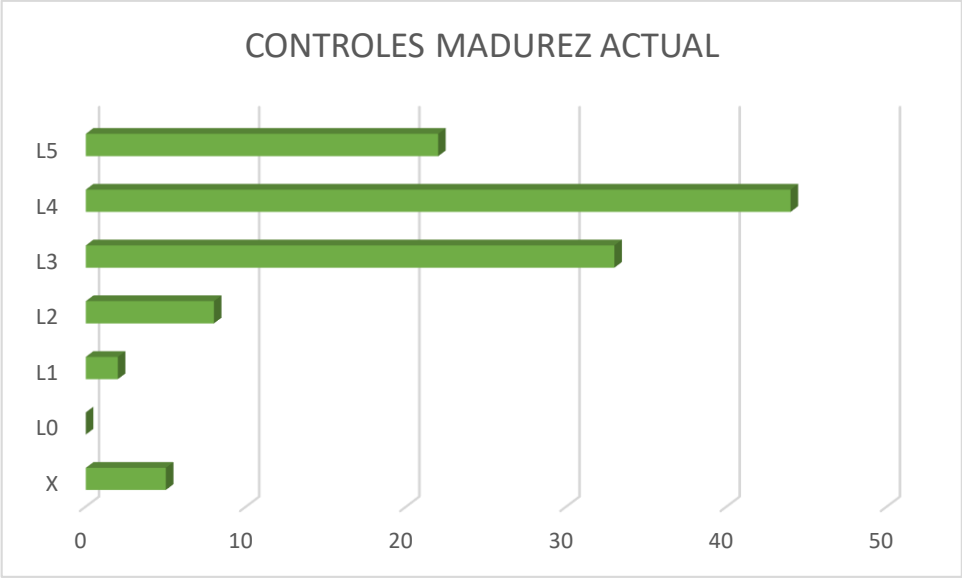

Ilustración 23: Número de controles A por estado CMM actual

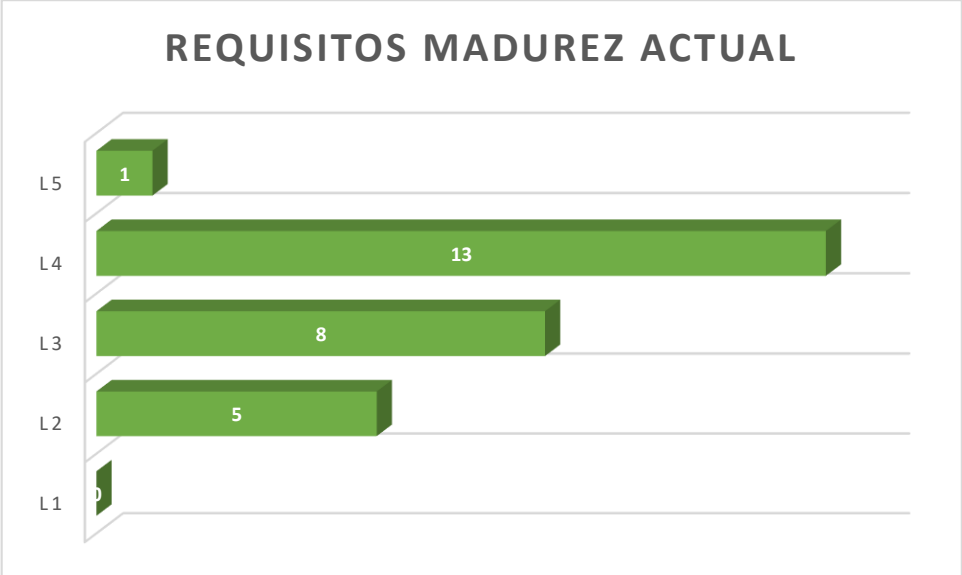

Ilustración 24: Número requerimientos de SI por estado CMM actual

5.4 CONCLUSIONES

Tal como se puede apreciar en las tablas y en los gráficos de la fase 5 de este documento, el contraste en comparación del estado inicial frente al estado actual del SGSI para la institución Unidad Educativa Salesiana Maria Auxiliadora es evidente.

Existe una variación en cuanto a los controles del anexo A y lo que establece el análisis en la ISO 27002, de un 46.31%, lo cual denota que los proyectos y las medidas tomadas frente a la seguridad de la información han dado el resultado esperado.

Considerando los requisitos que establece la ISO 27001 para la seguridad de la información existe una mejora del 59.05%, esto demuestra que la institución ha tomado las medidas necesarias para superar la arcaica situación inicial frente a la seguridad informática.

A pesar de las notables mejoras de seguridad en la UESMA es menester indicar que la tecnología avanza y siempre pueden surgir nuevos inconvenientes o no se ha logrado cubrir en su totalidad los diferentes controles que establece la ISO 27002 y los requisitos de la ISO 27001, es por ello que, aunque quizás no es una no conformidad, se realizan diferentes comentarios en algunos de estos parámetros considerando los valores de la siguiente tabla.

Tipo de comentario	Descripción
No conformidad mayor	Incumplimiento completo del apartado normativo de control
No conformidad menor	Incumplimiento parcial del apartado normativo de control
Observación	No es una no conformidad pero si no se corrige podría pasar a ser una no conformidad menor
Punto de mejora	Es una recomendación que podría aportar mayor madurez

Tabla 46: Tipos de comentarios en controles

De manera consecutiva se muestra la tabla con los aspectos que han sido detectados con necesidad de algún tipo de comentario, los que no aparezcan se considera que tiene un muy buen nivel.

N°	Sección	Controles Seguridad de la Información	Control / Requerimiento	**TIPO COMENTARIO**	SUGERENCIA
1	A6	Organización de la seguridad de la información	A6.2.2	Punto de mejora	Se recomienda dar mayor realce al teletrabajo puesto que se evidencia la necesidad de esta forma de trabajar por varios funcionarios de la UESMA

2	A8	Gestión de activos	A8.1.4	No conformidad menor	Es importante que se realice seguimiento a los activos que se disponen a ser usados fuera de la institución puesto que esta actividad es frecuenta en la institución y por los índices son vulnerables a perdidas y/o inconsistencias en los mismos. Además a los empleados que cesen sus funciones es necesario que aunque los dispositivos de almacenamiento extraíbles queden con ellos, realizar una verificación de la información que contiene.
3	A9	Control de acceso	A9.2.6	Observación	Aunque no es posible acceder desde fuera de la red LAN es necesario que se desactiven los usuarios que han cesado funciones de los sistemas de información.
4	A15	Relación con proveedores	A15.2.1	Observación	Los documentos como contratos, acuerdos, etc, entre los proveedores y la institución deben tener un realce legislativo
		Requisitos ISO 27001			
5	5	Liderazgo	5.1	Punto de mejora	Los directivos han demostrado un gran compromiso con la seguridad pero es importante su mayor participación en las reuniones del comité de seguridad y los informes sin delegar funciones.
6	7	Soporte	7.1	No conformidad menor	Se evidenció que las personas que forman parte del equipo de seguridad de la información cumplen roles extras en la institución que podrían absorber mucho tiempo que debería dedicarse a lo que el rol demanda.

Tabla 47: Comentarios Requerimientos ISO 27001

FASE 6: RESULTADOS

Minimizar el riesgo en torno al C.I.D.A.T

C.I.D.A.T, criterios tomados como referencia para el análisis de riesgos e impacto potencial. Los activos contemplados en el SGSI en la actualidad se garantiza la seguridad de los mismos en cuanto a confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad, lo cual genera el mayor aporte y el de más realce para la seguridad de la información.

Mejora continua de la seguridad de la información.

La metodología usada, conocida como el ciclo de Demming permite una actualización constante en los parámetros de seguridad de la información y el Sistema Gestor de Seguridad en General, siendo este un aporte importante para la UESMA en vista que de manera periódica se realizan adquisiciones de activos de información y relacionados.

Mayor tiempo de productividad.

Con la optimización de la seguridad y la implementación del plan de continuidad de negocio, para la institución es posible mantenerse mayor tiempo productiva puesto que existen alternativas de los principales procesos frente a la ocurrencia de una amenaza que altere el funcionamiento normal de la UESMA, disminuyendo también el riesgo de afectación de los activos.

Mejores garantías a los clientes y personal de la UESMA.

Gracias al SGSI es posible garantizar la seguridad de los datos y también de procesos relacionados con estos, lo cual otorga a los clientes y empleados una mejor garantía sobre la custodia y cuidados de sus datos personales.

Optimización de recursos y costos.

Con la mitigación de riesgos se garantiza que los recursos disponibles se usen de manera adecuada para evitar la degradación de los mismos por actividades no relacionadas con la institución, así como también de los responsables de los mismos, lo cual se refleja en una reducción de costos destinados a reparación y reposición de los mismos.

Garantías legales.

La realización de este proyecto ha permitido a la institución conocer y basarse en varios documentos legales como leyes, reglamentos, códigos y otros que permiten un respaldo jurídico frente a situaciones contractuales en diversos casos con los empleados, incluso

posterior al cese de sus funciones, así como también corregir procesos que violentaban alguno de los documentos mencionados relacionados con clientes y personal que labora en la institución.

Inventario de activos.

Conocer exactamente los activos de información y los responsables de cada uno de estos ha sido una de las labores realizada en el SGSI, esto permite a la institución un mejor manejo de los recursos y establecer un reglamento de pertenencia, uso y movilidad de los mismos para evitar pérdidas y malfuncionamientos de los mismos sin responsables directos.

Mejor competitividad.

Al ser una institución preocupada por la seguridad de la información, así como los datos de los clientes y empleados brinda una motivación extra a estos mismos que dan testimonio de la situación frente a la seguridad, brindando a la UESMA mayor credibilidad y garantías de calidad frente a otras instituciones del mismo tipo de la localidad.

Referencias bibliográficas

Módulos de la materia “Trabajo Final de master de la UOC”

ISO 27001

ISO 27002

MAGERIT

https://whatis.techtarget.com/definition/ISO-27001

https://www.iso.org/standard/54533.html

http://www.iso27000.es/download/doc_sgsi_all.pdf

https://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/

https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

http://seguridadinformaica.blogspot.com/p/analisis-de-riesgo.html

http://www.iimv.org/iimv-wp-1-0/resources/uploads/2015/01/CNBSAuditoria.pdf

ANEXOS

ANEXO I: Informe de auditoría interna

INFORME DE AUDITORIA INTERNA			
Código:	AIU##-"AÑO"	**Tipo:**	Total/Parcial
Área:	(Sistema información/ proceso)	**Fecha:**	dd/mm/aaaa
Elaborado por	**Revisado por**	**Aprobado por**	
Objetivo:			
Resultados			
No conformidad		**Recomendaciones**	
Observaciones		**Conclusiones**	
Firma auditor		**Firma responsable Sistema o proceso**	

ANEXO II: Análisis de madurez del Anexo A

Sección	Controles Seguridad de la Información	ACTUAL		INICIAL	
		CMM	%	CMM	%
A5	**Políticas de seguridad de la información**	**L4**	**81.00%**	**L0**	**3.00%**
A5.1	**Directrices de gestión de la seguridad de la información**	**L4**	**81.00%**	**L0**	**3.00%**
A5.1.1	Políticas para la seguridad de la información	L4	87.00%	L0	6.00%
A5.1.2	Revisión de las políticas para la seguridad de la información	L3	75.00%	L0	0.00%
A6	**Organización de la seguridad de la información**	**L3**	**79.70%**	**L1**	**11.80%**
A6.1	**Organización interna**	**L3**	**76.40%**	**L1**	**7.60%**
A6.1.1	Roles y responsabilidades en seguridad de la información	L4	85.00%	L1	9.00%
A6.1.2	Segregación de tareas	L2	68.00%	L1	7.00%
A6.1.3	Contacto con las autoridades	L3	78.00%	L1	8.00%
A6.1.4	Contacto con grupos de interés especial	L3	75.00%	L1	6.00%
A6.1.5	Seguridad de la información en la gestión de proyectos	L3	76.00%	L1	8.00%
A6.2	**Los dispositivos móviles y el teletrabajo**	**L4**	**83.00%**	**L1**	**16.00%**
A6.2.1	Política de dispositivos móviles	L4	88.00%	L2	32.00%
A6.2.2	Teletrabajo	L3	78.00%	L0	0.00%
A7	**Seguridad relativa a los recursos humanos**	**L5**	**90.22%**	**L0**	**6.17%**
A7.1	**Antes del empleo**	**L5**	**93.00%**	**L0**	**7.50%**
A7.1.1	Investigación de antecedentes	L5	95.00%	L0	6.00%
A7.1.2	Términos y condiciones del empleo	L5	91.00%	L0	9.00%
A7.2	**Durante el empleo**	**L4**	**92.67%**	**L0**	**11.00%**
A7.2.1	Responsabilidades de gestión	L5	94.00%	L0	8.00%
A7.2.2	Concienciación, educación y capacitación en seguridad de la información	L5	93.00%	L1	18.00%

A7.2.3	Proceso disciplinario	L3	91.00%	L0	7.00%
A7.3	**Finalización del empleo o cambio en el puesto de trabajo**	**L4**	**85.00%**	**L0**	**0.00%**
A7.3.1	Responsabilidades ante la finalización o cambio	L4	85.00%	L0	0.00%
A8	**Gestión de activos**	**L3**	**71.03%**	**L1**	**37.67%**
A8.1	**Responsabilidad sobre los activos**	**L4**	**83.75%**	**L2**	**44.00%**
A8.1.1	Inventario de activos	L5	98.00%	L3	71.00%
A8.1.2	Propiedad de los activos	L3	75.00%	L2	53.00%
A8.1.3	Uso aceptable de los activos	L3	78.00%	L1	18.00%
A8.1.4	Devolución de activos	L4	84.00%	L1	34.00%
A8.2	**Clasificación de la información**	**L3**	**75.00%**	**L1**	**45.00%**
A8.2.1	Clasificación de la información	L3	75.00%	L1	45.00%
A8.2.2	Etiquetado de la información	L2	68.00%	L0	9.00%
A8.2.3	Manipulado de la información	L3	71.00%	L1	32.00%
A8.3	**Manipulación de los soportes**	**L2**	**54.33%**	**L1**	**24.00%**
A8.3.1	Gestión de soportes extraíbles	L3	78.00%	L1	28.00%
A8.3.2	Eliminación de soportes	L1	20.00%	L0	7.00%
A8.3.3	Soportes físicos en tránsito	L2	65.00%	L1	37.00%
A9	**Control de acceso**	**L3**	**75.19%**	**L1**	**12.18%**
A9.1	**Requisitos de negocio para el control de acceso**	**L4**	**85.00%**	**L1**	**11.00%**
A9.1.1	Política de control de acceso	L3	75.00%	L0	8.00%
A9.1.2	Acceso a las redes y a los servicios de red	L5	95.00%	L1	14.00%
A9.2	**Gestión de acceso de usuario**	**L3**	**67.17%**	**L0**	**9.33%**
A9.2.1	Registro y baja de usuario	L2	65.00%	L0	7.00%
A9.2.2	Provisión de acceso de usuario	L3	78.00%	L1	17.00%
A9.2.3	Gestión de privilegios de acceso	L3	75.00%	L0	6.00%
A9.2.4	Gestión de la información secreta de autenticación de los usuarios	L3	78.00%	L0	8.00%
A9.2.5	Revisión de los derechos de acceso de usuario	L2	55.00%	L1	14.00%
A9.2.6	Retirada o reasignación de los derechos de acceso	L2	52.00%	L0	4.00%

A9.3	**Responsabilidades del usuario**	**L4**	**85.00%**	**L0**	**3.00%**
A9.3.1	Uso de la información secreta de autenticación	L4	85.00%	L0	3.00%
A9.4	**Control de acceso a sistemas y aplicaciones**	**L2**	**63.60%**	**L0**	**25.40%**
A9.4.1	Restricción del acceso a la información	L3	78.00%	L2	51.00%
A9.4.2	Procedimientos seguros de inicio de sesión	L3	73.00%	L1	14.00%
A9.4.3	Sistema de gestión de contraseñas	L2	56.00%	L0	7.00%
A9.4.4	Uso de utilidades con privilegios del sistema	L2	56.00%	L1	20.00%
A9.4.5	Control de acceso al código fuente de los programas	L3	55.00%	L1	35.00%
A10	**Criptografía**	**L2**	**63.50%**	**L0**	**4.50%**
A10.1	**Controles criptográficos**	**L2**	**63.50%**	**L0**	**4.50%**
A10.1.1	Política de uso de los controles criptográficos	L1	49.00%	L0	2.00%
A10.1.2	Gestión de claves	L3	78.00%	L0	7.00%
A11	**Seguridad física y del entorno**	**L5**	**92.72%**	**L2**	**64.19%**
A11.1	**Áreas seguras**	**L5**	**93.00%**	**L3**	**73.83%**
A11.1.1	Perímetro de seguridad física	L5	97.00%	L3	78.00%
A11.1.2	Controles físicos de entrada	L5	95.00%	L2	59.00%
A11.1.3	Seguridad de oficinas, despachos y recursos	L4	87.00%	L3	75.00%
A11.1.4	Protección contra las amenazas externas y ambientales	L5	98.00%	L4	84.00%
A11.1.5	El trabajo en áreas seguras	L5	96.00%	L3	76.00%
A11.1.6	Áreas de carga y descarga	L4	85.00%	L3	71.00%
A11.2	**Seguridad de los equipos**	**L5**	**92.44%**	**L2**	**54.56%**
A11.2.1	Emplazamiento y protección de equipos	L5	97.00%	L2	61.00%
A11.2.2	Instalaciones de suministro	L5	95.00%	L3	78.00%
A11.2.3	Seguridad del cableado	L5	98.00%	L3	79.00%
A11.2.4	Mantenimiento de los equipos	L5	95.00%	L3	75.00%

A11.2.5	Retirada de materiales propiedad de la empresa	L3	75.00%	L1	45.00%
A11.2.6	Seguridad de los equipos fuera de las instalaciones	L4	88.00%	L1	48.00%
A11.2.7	Reutilización o eliminación segura de equipos	L5	95.00%	L1	44.00%
A11.2.8	Equipo de usuario desatendido	L5	97.00%	L1	22.00%
A11.2.9	Política de puesto de trabajo despejado y pantalla limpia	L5	92.00%	L1	39.00%
A12	**Seguridad de las operaciones**	**L4**	**86.85%**	**L2**	**59.39%**
A12.1	**Procedimientos y responsabilidades operacionales**	**L4**	**82.33%**	**L1**	**13.33%**
A12.1.1	Documentación de procedimientos operacionales	L4	82.00%	L1	11.00%
A12.1.2	Gestión de cambios	L4	84.00%	L1	14.00%
A12.1.3	Gestión de capacidades	L4	81.00%	L1	15.00%
A12.1.4	Separación de los recursos de desarrollo, prueba y operación	X	X	X	X
A12.2	**Protección contra el software malicioso (malware)**	**L5**	**97.00%**	**L3**	**70.00%**
A12.2.1	Controles contra el código malicioso	L5	97.00%	L3	70.00%
A12.3	**Copias de seguridad**	**L5**	**94.00%**	**L2**	**51.00%**
A12.3.1	Copias de seguridad de la información	L5	94.00%	L2	51.00%
A12.4	**Registros y supervisión**	**L4**	**85.75%**	**L2**	**60.00%**
A12.4.1	Registro de eventos	L4	83.00%	L1	49.00%
A12.4.2	Protección de la información del registro	L4	92.00%	L2	68.00%
A12.4.3	Registros de administración y operación	L3	82.00%	L1	44.00%
A12.4.4	Sincronización del reloj	L4	86.00%	L3	79.00%
A12.5	**Control del software en explotación**	**X**	**#¡VALOR!**	**X**	**X**
A12.5.1	Instalación del software en explotación	X	X	X	X

A12.6	**Gestión de la vulnerabilidad técnica**	**L4**	**83.00%**	**L2**	**83.00%**
A12.6.1	Gestión de las vulnerabilidades técnicas	L4	80.00%	L2	80.00%
A12.6.2	Restricción en la instalación de software	L4	86.00%	L2	86.00%
A12.7	**Consideraciones sobre la auditoria de sistemas de información**	**L3**	**79.00%**	**L1**	**79.00%**
A12.7.1	Controles de auditoría de sistemas de información	L3	79.00%	L1	79.00%
A13	**Seguridad de las comunicaciones**	**L4**	**85.83%**	**L1**	**35.46%**
A13.1	**Gestión de la seguridad de las redes**	**L4**	**88.67%**	**L2**	**60.67%**
A13.1.1	Controles de red	L5	93.00%	L3	73.00%
A13.1.2	Seguridad de los servicios de red	L4	89.00%	L2	57.00%
A13.1.3	Segregación en redes	L4	84.00%	L2	52.00%
A13.2	**Intercambio de información**	**L3**	**83.00%**	**L1**	**10.25%**
A13.2.1	Políticas y procedimientos de intercambio de información	L4	82.00%	L1	12.00%
A13.2.2	Acuerdos de intercambio de información	L3	78.00%	L1	12.00%
A13.2.3	Mensajería electrónica	L4	87.00%	L1	17.00%
A13.2.4	Acuerdos de confidencialidad o no revelación	L3	85.00%	L0	0.00%
A14	**Adquisición, desarrollo y mantenimiento de los sistemas de información**	**L4**	**83.72%**	**L2**	**63.56%**
A14.1	**Requisitos de seguridad en los sistemas de información**	**L4**	**83.00%**	**L2**	**66.00%**
A14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	L4	87.00%	L1	42.00%
A14.1.2	Asegurar los servicios de aplicaciones en redes públicas	L3	74.00%	L2	79.00%
A14.1.3	Protección de las transacciones de servicios de aplicaciones	L4	88.00%	L2	77.00%

A14.2	**Seguridad en el desarrollo y en los procesos de soporte**	**L4**	**87.17%**	**L2**	**69.67%**
A14.2.1	Política de desarrollo seguro	X	X	X	X
A14.2.2	Procedimiento de control de cambios en sistemas	L4	87.00%	L2	68.00%
A14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	L4	84.00%	L1	45.00%
A14.2.4	Restricciones a los cambios en los paquetes de software	L4	89.00%	L2	77.00%
A14.2.5	Principios de ingeniería de sistemas seguros	L4	83.00%	L2	66.00%
A14.2.6	Entorno de desarrollo seguro	X	X	X	X
A14.2.7	Externalización del desarrollo de software	X	X	X	X
A14.2.8	Pruebas funcionales de seguridad de sistemas	L4	87.00%	L3	78.00%
A14.2.9	Pruebas de aceptación de sistemas	L5	93.00%	L4	84.00%
A14.3	**Datos de prueba**	**L4**	**81.00%**	**L2**	**55.00%**
A14.3.1	Protección de los datos de prueba	L4	81.00%	L2	55.00%
A15	**Relación con proveedores**	**L3**	**78.58%**	**L2**	**65.50%**
A15.1	**Seguridad en las relaciones con proveedores**	**L3**	**74.67%**	**L2**	**59.00%**
A15.1.1	Política de seguridad de la información en las relaciones con los proveedores	L3	71.00%	L2	57.00%
A15.1.2	Requisitos de seguridad en contratos con terceros	L4	81.00%	L3	76.00%
A15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	L3	72.00%	L1	44.00%
A15.2	**Gestión de la provisión de servicios del proveedor**	**L4**	**82.50%**	**L3**	**72.00%**
A15.2.1	Control y revisión de la provisión de servicios del proveedor	L4	84.00%	L3	73.00%
A15.2.2	Gestión de cambios en la provisión del servicio del proveedor	L4	81.00%	L3	71.00%

A16	**Gestión de incidentes de seguridad de la información**	**L4**	**84.57%**	**L2**	**52.29%**
A16.1	**Gestión de incidentes de seguridad de la información y mejoras**	**L4**	**84.57%**	**L2**	**52.29%**
A16.1.1	Responsabilidades y procedimientos	L5	92.00%	L1	47.00%
A16.1.2	Notificación de los eventos de seguridad de la información	L4	89.00%	L1	44.00%
A16.1.3	Notificación de puntos débiles de la seguridad	L4	85.00%	L1	48.00%
A16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	L4	85.00%	L2	59.00%
A16.1.5	Respuesta a incidentes de seguridad de la información	L4	87.00%	L2	66.00%
A16.1.6	Aprendizaje de los incidentes de seguridad de la información	L4	83.00%	L3	79.00%
A16.1.7	Recopilación de evidencias	L3	71.00%	L1	23.00%
A17	**Aspectos de seguridad de la información para la gestión de la continuidad de negocio**	**L4**	**82.50%**	**L2**	**55.33%**
A17.1	**Continuidad de la seguridad de la información**	**L3**	**78.00%**	**L1**	**31.67%**
A17.1.1	Planificación de la continuidad de la seguridad de la información	L3	76.00%	L0	4.00%
A17.1.2	Implementar la continuidad de la seguridad de la información	L4	84.00%	L1	47.00%
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	L3	74.00%	L1	44.00%
A17.2	**Redundancias**	**L4**	**87.00%**	**L3**	**79.00%**
A17.2.1	Disponibilidad de los recursos de tratamiento de la información	L4	87.00%	L3	79.00%
A18	**Cumplimiento**	**L4**	**82.50%**	**L1**	**18.50%**
A18.1	**Cumplimiento de los requisitos legales y contractuales**	**L3**	**80.00%**	**L1**	**29.00%**

A18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	L3	79.00%	L0	5.00%
A18.1.2	Derechos de Propiedad Intelectual (DPI)	L3	77.00%	L0	7.00%
A18.1.3	Protección de los registros de la organización	L4	85.00%	L3	78.00%
A18.1.4	Protección y privacidad de la información de carácter personal	L4	87.00%	L2	55.00%
A18.1.5	Regulación de los controles criptográficos	L3	72.00%	L0	0.00%
A18.2	**Revisiones de la seguridad de la información**	**L4**	**85.00%**	**L0**	**8.00%**
A18.2.1	Revisión independiente de la seguridad de la información	L4	84.00%	L0	7.00%
A18.2.2	Cumplimiento de las políticas y normas de seguridad	L4	86.00%	L0	3.00%
A18.2.3	Comprobación del cumplimiento técnico	L4	85.00%	L1	14.00%
	TOTAL	L4	81.69%	L1	37.94%

Tabla 48: Anexo 1 Controles Anexo A, CMM

ANEXO III: Análisis de madurez de requisitos de seguridad

Sección	Requerimientos ISO 27001	ACTUAL		INICIAL	
		CMM	%	CMM	%
4	**Contexto de la organización**	**L3**	**79.88%**	**L0**	**9.50%**
4.1	**Comprensión de la organización y de su contexto**	**L3**	**78.00%**	**L0**	**6.00%**
4.1	Determinar los objetivos del SGSI de la organización y cualquier problema que pueda afectar su eficacia	L3	78.00%	L0	6.00%
4.2	Comprensión de las necesidades y expectativas de las partes interesadas	L3	71.50%	L1	32.00%
4.2 (a)	**Identificar las partes interesadas incluyendo leyes aplicables, regulaciones, contratos, etc.**	**L2**	**68.00%**	**L0**	**32.00%**
4.2 (b)	**Determinar los requerimientos y obligaciones relevantes de seguridad de la información**	**L3**	**75.00%**	**L1**	**32.00%**
4.3	Determinación del alcance del SGSI	L4	88.00%	L0	0.00%
4.3	Determinar y documentar el alcance del SGSI	L4	88.00%	L0	0.00%
4.4	SGSI		82.00%	L0	0.00%
4.4	Establecer, implementar, mantener y mejorar de forma continua el SGSI acorde al estándar	L4	82.00%	L0	0.00%
5	Liderazgo	L3	76.67%	L1	30.67%
5.1	**Liderazgo y compromiso**	**L2**	**62.00%**	**L1**	**32.00%**
5.1	La administración debe demostrar liderazgo y compromiso por el SGSI	L2	62.00%	L1	32.00%

5.2	Política	L4	90.00%	L0	8.00%
5.2	**Documentar la Política de Seguridad de la Información**	**L4**	**90.00%**	**L0**	**8.00%**
5.3	**Roles, responsabilidades y autoridades en la organización**	**L3**	**78.00%**	**L1**	**52.00%**
5.3	Asignar y comunicar los roles y responsabilidades de seguridad de la información	L3	78.00%	L1	52.00%
6	Planificación	L4	83.50%	L1	19.17%
6.1	**Acciones para tratar los riesgos y oportunidades**	**L4**	**89.00%**	**L1**	**38.33%**
6.1.1	Diseñar el SGSI para satisfacer los requerimientos, tratando riesgos e identificando oportunidades	L5	95.00%	L0	8.00%
6.1.2	Definir e implementar un proceso de análisis de riesgos de seguridad de la información	L4	88.00%	L2	53.00%
6.1.3	Documentar e implementar un proceso de tratamiento de riesgos de seguridad de la información	L4	84.00%	L1	54.00%
6.2	**Objetivos de seguridad de la información y planificación para su consecución**	**L3**	**78.00%**	**L0**	**0.00%**
6.2	Establecer y documentar los planes y objetivos de la seguridad de la información	L3	78.00%	L0	0.00%
7	**Soporte**	**L3**	**74.47%**	**L1**	**13.80%**
7.1	**Recursos**	**L2**	**58.00%**	**L1**	**13.00%**
7.1	Determinar y asignar los recursos necesarios para el SGSI	L2	58.00%	L1	13.00%
7.2	Competencia	L3	75.00%	L0	0.00%
7.2	Determinar, documentar hacer disponibles las competencias necesarias	L3	75.00%	L0	0.00%

7.3	Concienciación	L4	85.00%	L1	14.00%
7.3	**Implementar un programa de concienciación de seguridad**	**L4**	**85.00%**	**L1**	**14.00%**
7.4	Comunicación	L3	75.00%	L1	42.00%
7.4	Determinar la necesidades de comunicación internas y externas relacionadas al SGSI	L3	75.00%	L1	42.00%
7.5	Información documentada	L3	79.33%	L0	0.00%
7.5.1	**Proveer documentación requerida por el estándar más la requerida por la organización**	**L4**	**88.00%**	**L0**	**0.00%**
7.5.2	Proveer un título, autor, formato consistente, revisión y aprobación a los documentos	L4	85.00%	L0	0.00%
7.5.3	Mantener un control adecuado de la documentación	L2	65.00%	L0	0.00%
8	Operación	L4	82.33%	L1	25.00%
8.1	**Planificación y control operacional**	**L4**	**87.00%**	**L0**	**0.00%**
8.1	**Planificar, implementar, controlar y documentar el proceso de gestión de riesgos del SGSI (Tratamiento de riesgos)**	**L4**	**87.00%**	**L0**	**0.00%**
8.2	Apreciación de los riesgos de seguridad de la información	L4	85.00%	L1	13.00%
8.2	Evaluar y documentar los riesgos de seguridad regularmente y cuando hay cambios	L4	85.00%	L1	13.00%
8.3	**Tratamiento de los riesgos de seguridad de la información**	**L3**	**75.00%**	**L2**	**62.00%**
8.3	Implementar un plan de tratamiento de riesgos y documentar los resultados	L3	75.00%	L2	62.00%
9	Evaluación del desempeño	L3	75.67%	L0	0.00%

9.1	Seguimiento, medición, análisis y evaluación	L4	85.00%	L0	0.00%
9.1	Realizar un seguimiento, medición, análisis y evaluación del SGSI y los controles	L4	85.00%	L0	0.00%
9.2	Auditoría interna	L4	82.00%	L0	0.00%
9.2	Planificar y realizar una auditoria interna del SGSI	L4	82.00%	L0	0.00%
9.3	**Revisión por la dirección**	**L2**	**60.00%**	**L0**	**0.00%**
9.3	La administración realiza una revisión periódica del SGSI	L2	60.00%	L0	0.00%
10	**Mejora**	**L4**	**81.50%**	**L1**	**42.50%**
10.1	No conformidad y acciones correctivas	L4	88.00%	L1	47.00%
10.1	Identificar, arreglar y reaccionar ante no conformidades para evitar su recurrencia documentando todas las acciones	L4	88.00%	L1	47.00%
10.2	Mejora continua	L3	75.00%	L1	38.00%
10.2	Mejora continua del SGSI	L3	75.00%	L1	38.00%
	TOTAL	L3	78.82%	L1	18.64%

Tabla 49: Anexo2, Requisitos de seguridad, CMM