2021

FACULTAD DE POSGRADOS

DISEÑO DEL PROGRAMA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA PRIVADA GRUPO SES

AUTOR

Juan Carlos Gómez Paspuel

AÑO

2021

FACULTAD DE POSGRADOS

DISEÑO DEL PROGRAMA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA PRIVADA GRUPO SES

_____

Autor

Juan Carlos Gómez Paspuel

Año

2021

FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

DISEÑO DEL PROGRAMA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA PRIVADA GRUPO SES

Trabajo de Titulación presentado en conformidad con los requisitos establecidos para optar por el título de MAGÍSTER EN GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

_____

Autor

Juan Carlos Gómez Paspuel

Año

2021

AGRADECIMIENTOS

Agradezco a mi madre, a mis abuelos, a mi esposa e hijos, que son mi mayor motivación, por su apoyo incondicional, para cumplir esta meta y a todos los docentes por sus conocimientos impartidos, he logrado cumplir un nuevo objetivo profesional.

DEDICATORIA

A mi madre, a mi esposa mi compañera de vida, a mis amados hijos y a toda mi familia quienes confiaron en mí, desde el primer momento que decide cumplir con este nuevo reto académico.

RESUMEN

El presente proyecto tiene como objetivo diseñar un sistema de gestión de seguridad de la información para la empresa privada Grupo SES, ya que actualmente no cuenta con este tipo de sistema por lo tanto se encuentra expuesta a las amenazas en su infraestructura tecnológica.

En la primera fase se realiza el diagnóstico de evaluación de la empresa sobre la gestión de la seguridad de la información utilizando las Normas Internacionales ISO 27001:2013 y el Anexo A de la ISO 27001:2013, referente a los controles de seguridad de la Información.

En la segunda fase se efectúa la clasificación de los tipos de información de la empresa con su respectiva valoración conforme su giro de negocio.

En la tercera fase se ejecuta la identificación y clasificación de los activos críticos de la información de la empresa mediante la metodología de análisis y gestión de riesgos MAGERIT versión 3.

En la cuarta fase se obtiene el análisis de amenazas y vulnerabilidades de los activos información críticos de la empresa.

En la quinta fase se determina las políticas de alto nivel con sus respectivos roles y responsabilidades conforme las áreas definidas en la empresa.

En la sexta fase se define el modelo operacional del sistema de seguridad de la información aplicable para la empresa conforme el análisis de las etapas anteriormente descritas.

En la séptima y última fase la empresa, tendrá un programa de gestión de seguridad de la información (SGSI) el cual incluye los planes acción y proyectos determinados para su implementación.

Por último, se determinar las conclusiones y recomendaciones conforme el desarrollo de las fases descritas en el presente documento.

ABSTRACT

The objective of this project is to design an information security management system for the private company Grupo SES, since it currently does not have this type of system, therefore it is exposed to threats in its technological infrastructure.

In the first phase, the company's evaluation diagnosis on information security management is carried out using International Standards ISO 27001: 2013 and Annex A of ISO 27001: 2013, referring to Information security controls.

In the second phase, the types of information of the company are classified with their respective valuation according to their line of business.

In the third phase, the identification and classification of the company's critical information assets is carried out using the MAGERIT version 3 risk analysis and management methodology.

In the fourth phase, the analysis of threats and vulnerabilities of the critical information assets of the company is obtained.

In the fifth phase, the high-level policies are determined with their respective roles and responsibilities according to the areas defined in the company.

In the sixth phase, the operational model of the information security system applicable to the company is defined according to the analysis of the previously described stages.

In the seventh and final phase, the company will have an information security management program (ISMS) which includes action plans and projects determined for its implementation.

Finally, the conclusions and recommendations will be determined according to the development of the phases described in this document.

ÍNDICE

Tabla de contenido

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

1. INTRODUCCIÓN

En la actualidad el activo más importante para toda empresa es la información que genera o administra, independientemente de sus actividades.

Los avances tecnológicos permiten asegurar y controlar la información en las empresas además de poder establecer marcos de referencia para la gestión de la seguridad de la información en las empresas.

En el caso preciso de la empresa privada Grupo SES, la información que se genera y administra, es considerada de alta importancia y su confidencialidad es posee importancia a todo nivel, por lo tanto, es necesario implementar un Sistema de Gestión de Seguridad de la Información, para garantizar el uso adecuado de los sistemas y servicios informáticos, con lo cual se logrará niveles de seguridad óptimos en el procesamiento de la información.

Este proyecto tiene como propósito definir un Sistema de Gestión de Seguridad de la Información (SGSI) para la oficina principal de la empresa Grupo SES, conforme las fases definidas para la operación correcta del mismo.

2. DESARROLLO DEL PROYECTO DE TITULACIÓN

2.1 Caso de Negocio

2.1.1 Resumen Ejecutivo

El presente proyecto presenta el Diseño del Programa de Sistema de Gestión de la Seguridad de la Información, para que la empresa Grupo SES, pueda realizar su implementación de forma adecuada, con el fin de mitigar los riesgos en los activos de información críticos.

El diseño del Sistema de Gestión de Seguridad de la Información establece un modelo de operación ordenado para identificar, proteger, detectar, responder, y recuperar la información de la empresa conforme sus objetivos misionales, aplicando las mejores prácticas para la gestión de la información, fundamentalmente en su confidencialidad, integridad y disponibilidad.

2.1.2 Introducción

La empresa Grupo SES es un Safety Enforcement Seguridad Vial S.A. (SES) es una empresa ecuatoriana que participa de forma activa en el desarrollo de soluciones empresariales para la seguridad vial, soluciones que tienen como objetivo educar, concientizar a la ciudadanía y salvar vidas mediante campañas de educación vial.

La empresa Grupo SES se encuentra siempre en continuo desarrollo de nuevas ideas para ofrecer soluciones innovadoras de seguridad y educación en materia vial, siendo ampliamente reconocida en la ejecución de proyectos y cumplimiento de los parámetros que la entidad contratante disponga.

2.1.3 Misión

La misión de la compañía es precautelar la vida de las personas por medio de la instalación de sistemas de control de tránsito y velocidad con la más alta tecnología, implementando procesos técnicos con personal altamente capacitado en la materia para asegurar la calidad en cada paso.

2.1.4 Visión

A mediano plazo, ser la empresa número uno en Ecuador y Latinoamérica en proyectos de concientización ciudadana y educación vial, apoyados con tecnología de última generación.

2.1.5 Objetivo General

Diseñar el Programa de Sistema de Gestión de la Seguridad de la Información, para que la empresa Grupo SES.

2.1.6 Objetivo Específicos

- Identificar las amenazas y posibles riesgos informáticos a los que se enfrenta la empresa
- Analizar las amenazas y vulnerabilidades, y establecer controles para minimizar los riesgos encontrados.
- Sugerir medidas de seguridad para preservar los activos informáticos de la empresa, con base a la confidencialidad, integridad y disponibilidad.
- Desarrollar el programa del sistema de gestión de seguridad de la información (SGSI), en la empresa y capacitar el personal designado.

2.1.7 Alcance

El presente proyecto consiste en el Diseño de un Sistema de Gestión de Seguridad de la Información, el mismo se desarrollara en la oficina matriz de la empresa Grupo SES, mediante un diagnóstico inicial de la gestión de la seguridad de la información, se seleccionará los activos de información críticos, los principales riesgos a mitigar, definición de la políticas de alto nivel, los proyectos y planes de mejora que deben implementarse para la operación correcta y adecuada de dicho programa.

2.1.8 Identificación y Descripción del problema

La empresa Grupo SES, dentro de su planificación no tiene definido un Sistema de Gestión de Seguridad de la Información, conforme a las necesidades y problemática actual para proteger los datos que administra, procesa y almacena.

La alta gerencia de la empresa considera que la información es un activo muy importante y considera como prioritario, gestionar de forma eficaz el almacenamiento, procesamiento y transmisión de la información. Por lo tanto, la implementación de un Sistema de Gestión de Seguridad de la Información, es primordial para asegurar sus sistemas y servicios informáticos.

2.1.9 Justificación

En nuestro país las empresas públicas y privadas han sido víctimas de ataques a sus sistemas informáticos, provocando el robo y perdida de información, generando perjuicios económicos altos. La ausencia de políticas, procedimientos y la aplicación de controles para proteger y asegurar la información son el factor principal de estos eventos.

Por lo tanto, es importante el diseño de un Sistema de Gestión de Seguridad de la Información, para proteger la información de la empresa y reducir los riesgos de perdida de información, incrementado su competitividad operativa y confianza de sus clientes corporativos.

2.1.10 Descripción de oportunidad

La gestión adecuada de la seguridad de la información permitirá la reducción de los diversos riesgos a los que está expuesta la organización, como es la perdida de información, la falta de disponibilidad, el robo de información, espionaje, ataques informáticos, entre otros y que permitan la continuidad y el buen funcionamiento de las diferentes áreas y procesos de la empresa Grupo SES.

2.1.11 Identificación de la solución

Para el diseño de un Sistema de Gestión de Seguridad de la Información, se definen las siguientes fases:

1. Diagnóstico del SGSI conforme la norma internacional ISO 27001:2013.
2. Evaluación de los controles mediante el Anexo A norma internacional ISO 27001:2013.
3. Identificación y clasificación de activos de información críticos.
4. Identificación de amenazas y vulnerabilidades de los activos de información críticos y gestión de riesgos.
5. Definición de políticas alto nivel de seguridad de la información.
6. Operación del SGSI.
7. Proyectos y planes de mejora.

2.1.12 Cronograma

Figura 1. Cronograma del Sistema de Gestión de Seguridad de la Información.

3. DIAGNÓSTICO INICIAL

El análisis inicial del sistema de seguridad de la información en la empresa Grupo SES, es conforme lo establecido en la norma internacional ISO/IEC 27001:2013, la cual permite realizar un diagnóstico de la gestión de seguridad de la información dentro de la estructura organizacional (Anexo 1).

Mediante el Anexo A de la norma ISO 27001 el cual consta de un catálogo de 114 controles de seguridad que la empresa debe seleccionar de acuerdo con su aplicabilidad. El conocimiento de los controles del Anexo A nos ayuda a comprender mejor el estado de que la seguridad de la información y su alcance sobre las áreas como Recursos Humanos, Gestión de Activos, Seguridad Física, Medio Ambiente, Seguridad en las Comunicaciones y Relación en la Cadena de Suministro (Anexo 2).

3.1 Estado inicial del SGSI

El diagnóstico del estado inicial del Sistema de Seguridad de la Información, en la empresa Grupo SES, se determina mediante la adaptación de los niveles de madurez para evaluar salvaguardas, según el modelo de madurez (CMM-Capability Maturity Model) usado para calificar la madurez de procesos conforme la Tabla 1.

Tabla 1.

Modelo Madurez.

Valor	Significado	Descripción
L0	**Inexistente**	No se lleva a cabo el control de seguridad en los sistemas de información.
L1	**Inicial**	Los controles existen, pero no se gestionan, no existe un proceso formal para realizarlas.
L2	**Repetible**	La medida de seguridad se realiza de un modo de responsabilidad individual. No hay formación de un plan.
L3	**Definido**	Se despliegan y se gestionan controles. Hay normativa establecida y procedimientos para garantizar la reacción profesional ante los incidentes.
L4	**Administrado**	El control se lleva a cabo de acuerdo a un procedimiento documentado, aprobado y formalizado por la alta gerencia.
L5	**Optimizado**	El control se aplica de acuerdo a un procedimiento documentado, aprobado y formalizado, y su eficacia se mide periódicamente mediante indicadores.

En la Tabla 2 se muestra el estado inicial del SGSI en la empresa SES.

Tabla 2.

Estado inicial SGSI.

Valor	Significado	Descripción	Eficacia	Porcentaje de cumplimiento Diagnóstico Inicial SGSI
L0	**Inexistente**	No se lleva a cabo el control de seguridad en los sistemas de información.	0%	0%
L1	**Inicial**	Los controles existen, pero no se gestionan, no existe un proceso formal para realizarlas.	10%	89%
L2	**Repetible**	La medida de seguridad se realiza de un modo de responsabilidad individual. No hay formación de un plan.	50%	0%
L3	**Definido**	Se despliegan y se gestionan controles. Hay normativa establecida y procedimientos para garantizar la reacción profesional ante los incidentes.	90%	11%
L4	**Administrado**	El control se lleva a cabo de acuerdo a un procedimiento documentado, aprobado y formalizado por la alta gerencia.	95%	0%
L5	**Optimizado**	El control se aplica de acuerdo a un procedimiento documentado, aprobado y formalizado, y su eficacia se mide periódicamente mediante indicadores.	100%	0%

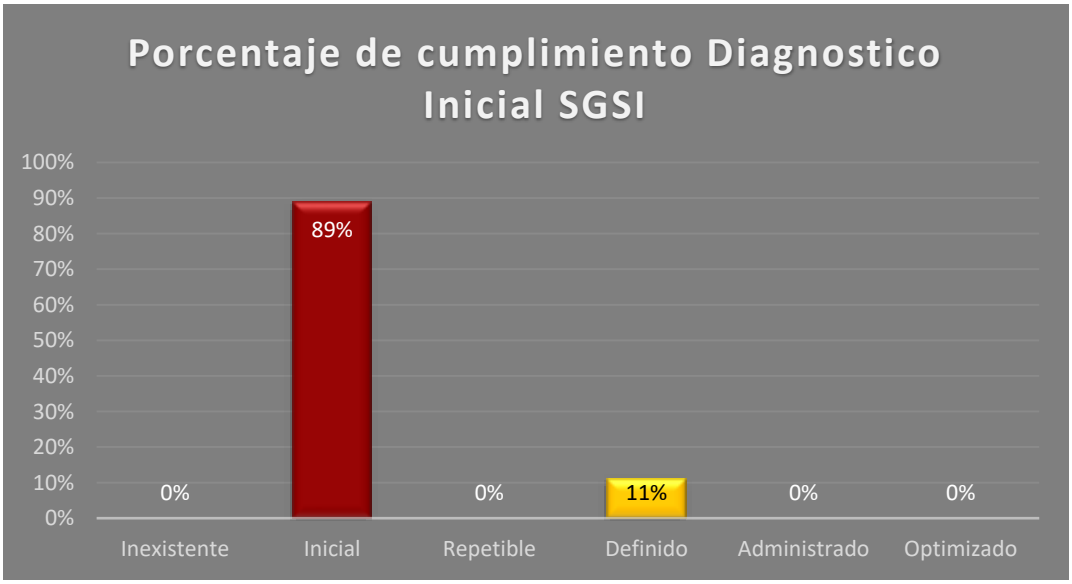


Figura 2. Diagnóstico del Sistema de Gestión de Seguridad de la Información.

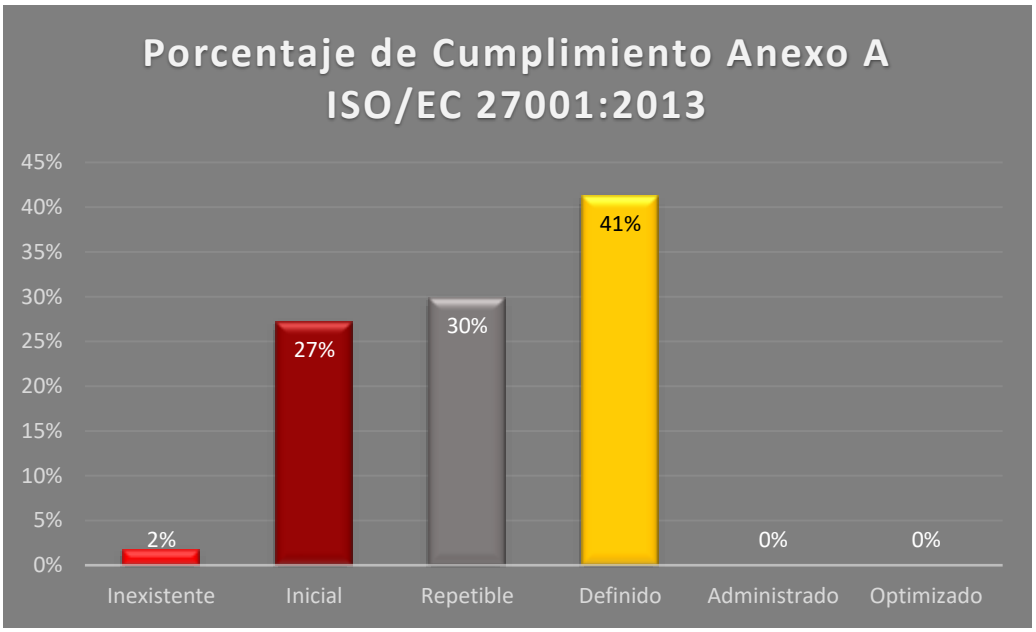


Figura 3. Porcentaje de cumplimiento Anexo A ISO 27001:2013.

Conforme la información obtenida de las tablas anteriores se determina que la empresa Grupo SES, debe iniciar de forma integral el Sistema de Gestión de Seguridad de la Información, ya que los resultados preliminares son bajos conforme el nivel de madurez establecido.

3.2. Diagnóstico de los Controles Anexo A ISO 27001:2013

La situación actual de la empresa Grupo SES se identifican en la siguiente tabla.

Tabla 3.

Evaluación Efectividad de Controles.

Evaluación de Efectividad de Controles Anexo A ISO 27001:2013				
No.	**DOMINIO**	**Estado Actual**	**Estado Objetivo**	**RESULTADO EFECTIVIDAD CONTROL**
A.5	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	90	95	**DEFINIDO**
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	61	95	**DEFINIDO**

A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	83	95	DEFINIDO
A.8	GESTIÓN DE ACTIVOS	62	95	DEFINIDO
A.9	CONTROL DE ACCESO	41	95	REPETIBLE
A.10	CRIPTOGRAFÍA	50	95	REPETIBLE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	62	81	DEFINIDO
A.12	SEGURIDAD DE LAS OPERACIONES	56	93	DEFINIDO
A.13	SEGURIDAD DE LAS COMUNICACIONES	90	95	DEFINIDO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	19	95	REPETIBLE
A.15	RELACIONES CON LOS PROVEEDORES	90	95	DEFINIDO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	44	94	REPETIBLE
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	10	95	INICIAL
A.18	CUMPLIMIENTO	55	93	DEFINIDO

De acuerdo con los resultados obtenidos en la Tabla 3, la Empresa SES tiene la mayoría de controles con su nivel madurez en estado definido, luego en estado Repetible y uno solo en estado inicial, por lo tanto, se deben mejorar los procesos y procedimientos en los controles conforme la Norma ISO 27001:2013.

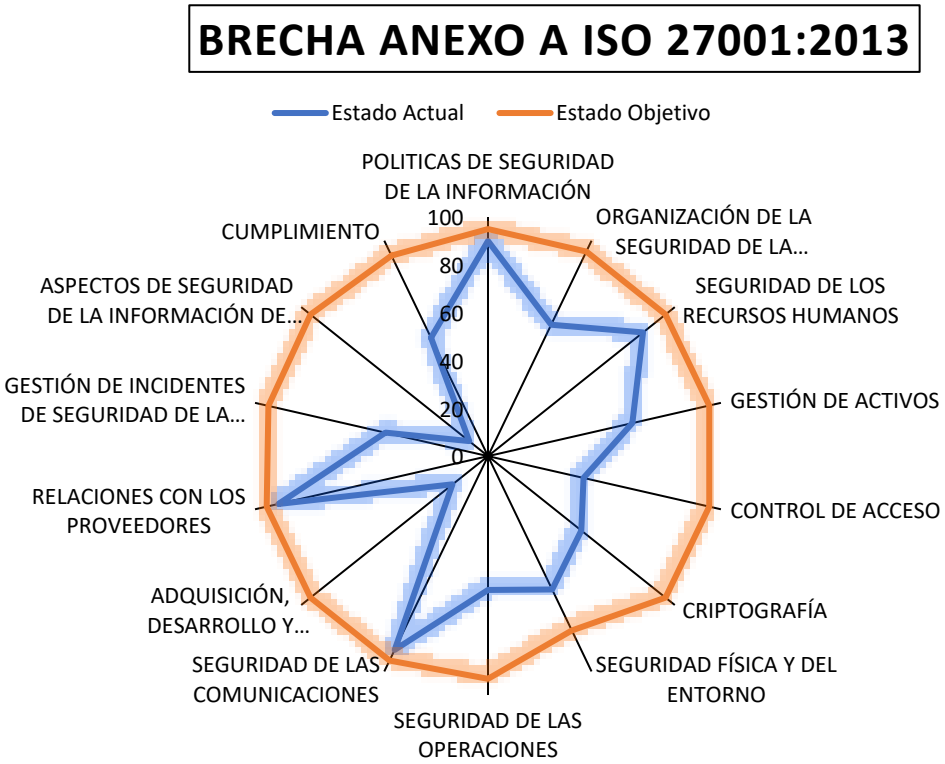


Figura 4. BRECHA ISO/IEC 27001:2013 Anexo A.

En la Figura 3, se identifica el estado actual y el estado objetivo de los controles de la Norma ISO 27001:2013.

3.3. Clasificación de la Información

Mediante un trabajo conjunto con el departamento de tecnología se realiza la clasificación de la información considerada importante para la empresa Grupo SES, a continuación, su clasificación:

Tabla 4.

Clasificación de Activos de Información.

No.	Nombre de la entidad	Nombre del tipo de información	Definición del tipo de información
1	**Municipio (GAD)**	Vehículo	Placa, Chasis, Marca, Modelo, Propietario, Cilindraje, Tipo de Servicio
2		Conductor	Cedula, Nombres, Apellidos, Email, Dirección
3		Matricula	Fecha de emisión, Lugar de emisión, Fecha de caducidad
4		Digitador	Nombres, Apellidos, Código, Rol
5		Multa	Fecha de infracción, Valor, Interés, Lugar, Estado (pagada, anulada, activa)

6	**Proveedor (Sistema Fotomultas)**	Vehículo	Placa
7		Imagen	Vehículo
8		Ubicación	Coordenadas, GPS
9		Tipo	Fijo, Móvil
10		Ciudad	Provincia, Cantón, Dirección
11	**Proveedor (Sistema Amazon AWS)**	Vehículo	Placa, Chasis, Marca, Modelo, Propietario, Cilindraje, Tipo de Servicio
12		Conductor	Cedula, Nombres, Apellidos, Email, Dirección
13		Fotomulta	Fecha de emisión, Lugar de emisión, Fecha de caducidad
14		Ubicación	Provincia, Cantón, Dirección
15		Digitador	Nombres, Apellidos, Código, Rol

La tabla anterior permite identificar los activos de información que deberán ser protegidos aplicando controles conforme la norma ISO 27001:2013.

3.4. Definición del modulador y niveles de Impacto

La definición del modulador y de los niveles de impacto, son importantes para identificar los activos de información críticos de la empresa Grupo SES, a continuación, su categorización:

Tabla 5.

Modulador Apetito del Riesgo.

IMPACTO		
Pérdidas financieras	Aversión	Mayor a 50.000
Pérdidas reputación	Aversión	Afectación a toda la empresa
Pérdida de la confidencialidad e integridad de la información	Agresivo	Número de incidentes de seguridad (confidencialidad e integridad)
Suspensión o pérdida total de los servicios electrónicos	Aversión	Número de incidentes de afectación del servicio
Fuga o robo de información de clientes	Neutral	Número Incidentes con información crítica

Tabla 6.

Niveles de Impacto.

Niveles

CATASTRÓFICO
MAYOR
MODERADO
MENOR
INSIGNIFICANTE

Como se mencionó anteriormente, la empresa Grupo SES, administra sistema de control de tránsito específicamente sistemas informáticos de Fotomultas siendo sus principales contratistas Gobiernos Autónomos Descentralizados del Estado Ecuatoriano, por lo tanto, la información que pertenece a dichas entidades es considera de muy alta importancia para su protección. A continuación, la tabla explicativa.

Tabla 7.

Categorización de la Información y sus niveles de Impacto.

No.	Nombre de la entidad	Nombre del tipo de información	Definición del tipo de información	Impacto con la Confidencialidad	Impacto con la Integridad	Impacto con la Disponibilidad	Impacto con la Privacidad	Calificación*
1	**Municipio (GAD)**	Vehículo	Placa, Chasis, Marca, Modelo, Propietario, Cilindraje, Tipo de Servicio	MODERADO	MODERADO	MODERADO	MODERADO	MODERADO
2		Conductor	Cedula, Nombres, Apellidos, Email, Dirección	MODERADO	MODERADO	MODERADO	MODERADO	MODERADO
3		Matricula	Fecha de emisión, Lugar de emisión, Fecha de caducidad	MODERADO	MODERADO	MODERADO	MODERADO	MODERADO
4		Digitador	Nombres, Apellidos, Código, Rol	MODERADO	MODERADO	MODERADO	MODERADO	MODERADO
5		Multa	Fecha de infracción, Valor, Interés, Lugar, Estado (pagada, anulada, activa)	MODERADO	MODERADO	MODERADO	MODERADO	MODERADO
6	**Proveedor (Sistema FotoMulta)**	Vehículo	Placa	MAYOR	MAYOR	MAYOR	MAYOR	CRITICO
7		Imagen	Vehículo	MAYOR	MAYOR	MAYOR	MAYOR	CRITICO
8		Ubicación	Coordenadas, GPS	MAYOR	MAYOR	MAYOR	MAYOR	CRITICO
9		Tipo	Fijo, Móvil	MAYOR	MAYOR	MAYOR	MAYOR	CRITICO

10		Ciudad	Provincia, Cantón, Dirección	MENOR	MENOR	MENOR	MENOR	MENOR
11	**Proveedor (Sistema Amazon AWS)**	Vehículo	Placa, Chasis, Marca, Modelo, Propietario, Cilindraje, Tipo de Servicio	MENOR	MENOR	MENOR	MENOR	MENOR
12		Conductor	Cedula, Nombres, Apellidos, Email, Dirección	MENOR	MENOR	MENOR	MENOR	MENOR
13		Fotomulta	Fecha de emisión, Lugar de emisión, Fecha de caducidad	MENOR	MENOR	MENOR	MENOR	MENOR
14		Ubicación	Provincia, Cantón, Dirección	MENOR	MENOR	MENOR	MENOR	MENOR
15		Digitador	Nombres, Apellidos, Código, Rol	MENOR	MENOR	MENOR	MENOR	MENOR

3.5. Inventario de activos de la información

Los activos de Información considerados críticos y de alto impacto en la empresa SES son los siguientes:

Tabla 8.

Inventarios de activos de Información.

Entidad	Nombre del Activo	Formato	Tipo de Activo	Responsable	Propietario
Oficina Principal	Servidores Virtuales AWS	Digital	Software	Jefe de Desarrollo	Grupo SES
	Servidores RDS / MySQL Community	Digital	Hardware	Jefe de Desarrollo	Grupo SES
	Servidor Local 1	Digital	Hardware	Jefe de Infraestructura	Grupo SES
	Servidor Local 2	Digital	Hardware	Jefe de Infraestructura	Grupo SES
	Servidor Local 3	Digital	Hardware	Jefe de Infraestructura	Grupo SES
	Servidor Almacenamiento	Digital	Hardware	Jefe de Infraestructura	Grupo SES
	Central Telefónica	Digital	Hardware	Jefe de Infraestructura	Grupo SES
	Enlace de Datos	Digital	Hardware	Jefe de Infraestructura	Grupo SES
	Enlace de Internet	Digital	Hardware	Jefe de Infraestructura	Grupo SES
	Router	Físico	Hardware	Jefe de Infraestructura	Grupo SES
	Swirtch	Físico	Hardware	Jefe de Infraestructura	Grupo SES
	Swirtch	Físico	Hardware	Jefe de Infraestructura	Grupo SES
	Swirtch	Físico	Hardware	Jefe de Infraestructura	Grupo SES
	Swirtch	Físico	Hardware	Jefe de Infraestructura	Grupo SES

	Firewall	Físico	Hardware	Jefe de Infraestructura	Grupo SES
	Firewall	Físico	Hardware	Jefe de Infraestructura	Grupo SES

3.6. Análisis de amenazas y vulnerabilidades

A continuación, se realiza el análisis de amenazas y vulnerabilidades de los activos considerados críticos dentro de la empresa Grupo SES, para esto es necesario determinar lo siguiente:

Tabla 9.

Niveles de Probabilidad.

PROBABILIDAD		
1	Raro	2 %
2	Poco probable	5 %
3	Posible	25 %
4	Probable	75 %
5	Casi Certeza	100 %

Tabla 10.

Niveles de Valoración del Impacto.

VALORACIÓN	
Casi Certeza	Catastrófico
Probable	Mayor
Posible	Moderado
Poco probable	Menor

Raro	Insignificante

Mediante la utilización del marco de referencia Magerit y la norma ISO 27005 se establecen las amenazas y vulnerabilidades, a las cuales están expuestos los activos de información críticos de la empresa Grupo SES, además del nivel de riesgo identificado.

Tabla 11.

Amenazas y Vulnerabilidades Activos de Información Críticos y nivel Riesgo.

Nombre de activo	Componentes	Amenaza MAGERIT	Vulnerabilidad ISO 27005	Probabilidad	Impacto	Riesgo
Sistema Fotomultas Matriz	[SW] Software	[I.5] Avería de origen lógico: Fallo en los programas	Defectos conocidos en el software	Probable	Mayor	Moderado
		[E.1] Errores de los usuarios: Equivocaciones de las personas	Falta de mecanismos de identificación y autentificación, como la autentificación de usuario	Raro	Mayor	Moderado
		[E.2] Errores del administrador: Equivocaciones de personas	Uso incorrecto de software	Raro	Mayor	Moderado
		[E.8] Difusión de software dañino: Malware	Conexiones de red pública sin protección	Probable	Mayor	Catastrófico
		[E.9] Errores de [re-]encaminamiento: Envío de información a través de un sistema incorrecto	Software nuevo e inmaduro	Raro	Moderado	Moderado

		[E.10] Errores de secuencia: Alteración accidental del orden de los mensajes	Especificaciones incompletas o no claras para los desarrolladores	Raro	Moderado	Moderado
		[E.19] Fugas de información: Robo o revelación de información	Servicios innecesarios habilitados	Posible	Moderado	Moderado
		[E.20] Vulnerabilidades de los programas (software): Defectos en el código	Software nuevo o inmaduro	Raro	Mayor	Moderado
		[E.21] Errores de mantenimiento / actualización de programas (software): Defectos o inexistencia de procedimientos o controles de actualización	Falta de control de cambios efectivo	Poco probable	Mayor	Mayor
		[A.5] Suplantación de la identidad del usuario: Phishing	Falta de mecanismos de identificación y autentificación, como la autentificación de usuario	Posible	Moderado	Moderado
		[A.11] Acceso no autorizado: Acceso a recursos del sistema sin tener autorización	Asignación incorrecta de derechos de acceso	Probable	Moderado	Catastrófico

	[HW] Equipamiento informático (hardware)	[N.1] Fuego: Incendio	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	Raro	Mayor	Moderado
		[N.2] Daños por agua: Escape o fuga	Susceptibilidad a la humedad	Raro	Mayor	Moderado
		[N.*] Desastres naturales: Terremoto	Ausencia de planes de continuidad	Raro	Mayor	Moderado
		[I.5] Avería de origen físico o lógico: Fallo o desconexión en los equipos	Mantenimiento insuficiente	Poco probable	Mayor	Mayor
		[I.6] Corte del suministro eléctrico: Corte de energía	Red energética inestable	Poco probable	Mayor	Mayor
		[I.7] Condiciones inadecuadas de temperatura o humedad: Fallo en sistema de climatización	Susceptibilidad a las variaciones de temperatura	Raro	Mayor	Moderado
		[E.2] Errores del administrador: Equivocaciones de personas	Falta de control de cambio con configuración eficiente	Probable	Mayor	Catastrófico
		[E.23] Errores de mantenimiento / actualización de equipos (hardware): Equipos utilizados más allá del tiempo nominal de uso, sin mantenimiento	Falta de esquemas de reemplazo periódico	Raro	Mayor	Moderado

		[E.24] Caída del sistema por agotamiento de recursos: Recursos insuficientes provoca la caída del sistema	Ausencia de esquemas de reemplazo periódico.	Poco probable	Mayor	Mayor
		[A.24] Denegación de servicio: Saturación de recursos	Falta de control de cambios de configuración eficiente	Poco probable	Mayor	Mayor
	[COM] Enlace de Internet	[I.8] Fallo de servicios de comunicaciones: Pérdida de servicio de comunicación	Arquitectura insegura de la red	Poco probable	Mayor	Mayor
		[E.9] Errores de [re-]encaminamiento: Envío de información a través de una red incorrecta	Gestión de red inadecuada	Raro	Moderado	Moderado
		[E.10] Errores de secuencia: Alteración accidental del orden de los mensajes	Tráfico sensible sin protección	Raro	Moderado	Moderado
		[E.19] Fugas de información: Robo o revelación de información	Líneas de comunicación desprotegidas	Probable	Moderado	Moderado
		[A.12] Análisis de tráfico: Monitorización de tráfico	Gestión inadecuada de la red (Tolerancia a fallas en el enrutamiento)	Raro	Moderado	Moderado

Tabla 12.

Mapa de Calificación del Riesgo.

MAPA DE CALIFICACIÓN SEVERIDAD DE RIESGO		
		IMPACTO

		INSIGNIFICANTE	MENOR	MODERADO	MAYOR	CATASTRÓFICO
Probabilidad	RARO	Bajo	Bajo	Moderado	Moderado	Alto
	POCO PROBABLE	Bajo	Bajo	Moderado	Alto	Alto
	POSIBLE	Bajo	Moderado	Moderado	Alto	Crítico
	PROBABLE	Bajo	Moderado	Alto	Crítico	Crítico
	CASI CERTEZA	Moderado	Moderado	Alto	Crítico	Crítico

3.7. Aplicación de Controles en las Dimensiones de Confidencialidad, Integridad y Disponibilidad.

En esta sección es relevante definir e identificar, de acuerdo al estándar ISO/IEC 27001, que la protección de los activos es salvaguardar la confidencialidad, la integridad y la disponibilidad de la información. Además, puede abarcar otras propiedades como la autenticidad, la responsabilidad y la fiabilidad. A continuación que significan cada uno de estos términos en relación con la información:

Confidencialidad: la información no se pone a disposición ni se revela a personas, entidades o procesos no autorizados.

Integridad: Mantener la exactitud y completitud de la información, es decir prevenir modificaciones no autorizadas de la información.

Disponibilidad: Garantizar el acceso y la utilización de la información, por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Una vez identificado los activos de información críticos es necesario aplicar los controles necesarios para salvaguardar su confidencialidad, integridad y disponibilidad.

Tabla 13.

Activos de Información Críticos Controles y Dimensiones CID.

Nombre de activo	Componentes	Controles ISO 27002	Dimensiones		
			Confidencialidad	Integridad	Disponibilidad
Sistema Fotomultas Matriz	[SW] Software	Gestión de vulnerabilidades técnicas	75%	5%	75%
		Establecer funciones y responsabilidades	75%	5%	25%
		Documentación de procedimientos de operación	75%	25%	5%
		Software Antimalware & EDR	75%	75%	100%
		Principios de ingeniería de sistemas seguros	75%	5%	25%
		Gestión de Versiones	75%	5%	25%
		Gestión de vulnerabilidades técnicas	75%	5%	25%
		Restricciones a los cambios en los paquetes de software	75%	5%	25%
		Gestión de cambios	75%	5%	25%

		Identificación y autenticación de usuario	75%	25%	5%
		Gestión de privilegios de acceso	100%	100%	100%
	[HW] Equipamiento informático (hardware)	Desarrollo e implantación de planes de continuidad	25%	25%	25%
		Protección contra amenazas externas y ambientales	25%	5%	25%
		Desarrollo e implantación de planes de continuidad	25%	25%	25%
		Mantenimiento del equipamiento	25%	5%	25%
		Desarrollo e implantación de planes de continuidad	25%	5%	25%
		Protección contra amenazas externas y ambientales	25%	5%	25%
		Prevención del uso indebido de recursos de tratamiento de la información	75%	100%	100%
		Mantenimiento del equipamiento	75%	5%	25%
		Mantenimiento de los equipos.	25%	75%	25%
		Gestión de vulnerabilidades técnicas	25%	5%	25%

	[COM] Enlace de Internet	Seguridad de los servicios de red	25%	5%	25%
		Controles de red	25%	5%	25%
		Seguridad de los servicios de red	25%	5%	25%
		Seguridad de los servicios de red	75%	75%	100%
		Segmentación de la red	75%	5%	25%

3.8. Políticas de Alto Nivel del Sistema de Seguridad de la Información.

Las Políticas de Alto nivel son importantes para el Sistema de Seguridad de la Información, la Dirección de Tecnologías de la empresa Grupo SES, será la encargada de su elaboración y su posterior aprobación por la Gerencia General, conforme el detalle de la siguiente tabla.

Tabla 14.

Políticas de Alto Nivel.

Definición	Objetivo	Alcance	Acciones
Política General de Seguridad de la Información	Establecer las medidas organizacionales, técnicas, físicas y legales, necesarias para proteger los activos de información contra acceso no autorizado, divulgación, duplicación, interrupción de sistemas, modificación, destrucción, pérdida, robo, o	Esta política es aplicable a todos los colaboradores, consultores, contratistas, terceras partes, que usen activos de información que sean propiedad de la organización.	1.Revisar la política de seguridad de la información. 2.Actualizar periódicamente la matriz de riesgos y el inventario de activos informáticos críticos. 3. Definir responsabilidades de los dueños de la información. 4.Sensibilizar la importancia de la política dentro de la Organización. 5. Asegurar el uso adecuado de los equipos y sistemas informáticos.

	mal uso, que se pueda producir en forma intencional o accidental		6. Garantizar la integridad, confidencialidad y disponibilidad de la información de la Organización. 7. Definir el uso adecuado de contraseñas de acceso. 8. Clasificar la información para identificar su valor y criticidad. 9. Aprobar la política de Seguridad de la Información.
Política de Control de Acceso	Establecer un adecuado control de acceso a los recursos y servicios tecnológicos de la Organización	Esta política es aplicable a todos los colaboradores, consultores, contratistas, terceras partes, que accedan a los activos de información que sean propiedad de la organización.	1. Identificación, verificación y asignación de permisos del usuario para uso de los sistemas, servicios informáticos de la organización. 2. Registro de usuarios autorizados. 3. Definición de roles y perfiles por cada sistema. 4. Acceso a los recursos de red. 5. Asignación de Privilegios. 6. Administración de contraseñas de usuarios. 7. Definición de actualización, eliminación y/o bloqueo del usuario. 8.Formulario de acceso para el usuario con las condiciones y sanciones definidas.

Política de Adquisición, Desarrollo y Mantenimiento de Aplicaciones Informáticas	Definir los lineamientos de seguridad en los sistemas de información para el correcto desempeño de los mismos considerando las buenas prácticas dentro del ciclo de vida para el desarrollo interno o adquisición de sistemas de informáticos.	Esta política controla la adquisición, desarrollo y mantenimiento de los sistemas de información de la organización	1. Establecer los requerimientos funcionales, no funcionales, técnicos y de seguridad en el desarrollo de sistemas. 2. Identificación de los controles que se deben implementar en los sistemas de información. 3. Definir los controles de validación de los datos de entrada, del procesamiento y los datos de salida. 4. Delimitar reglas del negocio que afecten las transacciones de la información o datos en las aplicaciones. 5. Detallar funciones y responsabilidades para el personal que participa en desarrollo, pruebas y pre-producción de los sistemas. 6. Establecer y generar pistas de auditoría de las transacciones en los sistemas. 7. Procedimientos para elaborar reportes automáticos. 8. Directrices para clasificar la información privada y confidencial. 9. Control de cambios sobre los sistemas. 10. Acceso a los ambientes de prueba y producción.
Política de Respaldo de Información	Proteger los datos, sistemas, aplicaciones y demás tipo de información que genera la organización y su recuperación en caso de fallas en su operación o manipulación.	Esta política es para toda la información que se encuentra almacenada en la infraestructura tecnológica que almacene o procese datos, sistemas y	1. Establecer las fuentes o bases de datos a respaldar. 2. Definir los tipos de respaldos para los sistemas de información. 3. Reglas de respaldo de las bases de datos. 4. Determinar la frecuencia y periodicidad de los respaldos.

		aplicaciones de la organización.	5. Codificación y clasificación de los respaldos. 6. Establecer puntos de restauración y acceso a los respaldos. 7. Planificar, ejecutar y monitorear pruebas de restauración de respaldos.

3.9. Operación del Programa del Sistema de Seguridad de la Información.

La Operación del programa del Sistema de Seguridad de la Información, se fundamenta en el marco de ciberseguridad NIST.

El Marco de ciberseguridad NIST, es conjunto de funciones y actividades de seguridad cibernética, consta de cinco funciones simultáneas y continuas: Identificar, Proteger, Detectar, Responder y Recuperar. Para este proyecto en particular, se consideran las que están dentro de la visión estratégica de alto nivel para la gestión de riesgos de la seguridad cibernética de la empresa

Tabla 15.

Modelo Operacional basado en NIST.

Función	Categoría	Subcategoría	Descripción Subcategoría
1. IDENTIFICAR	1. Gestión de activos (ID.AM)	ID.AM-1	Los dispositivos y sistemas físicos dentro de la organización están inventariados.
	3. Gobernanza (ID.GV)	ID.GV-1	Se establece y se comunica la política de seguridad cibernética organizacional.
	4. Evaluación de riesgos (ID.RA)	ID.RA-1	Se identifican y se documentan las vulnerabilidades de los activos.
2. PROTEGER	1. Gestión de identidad, autenticación y control de acceso (PR.AC)	PR.AC-1	Las identidades y credenciales se emiten, se administran, se verifican, se revocan y se auditan para los dispositivos, usuarios y procesos autorizados.

	2. Concienciación y capacitación (PR.AT)	PR.AT-1	Todos los usuarios están informados y capacitados.
	4. Procesos y procedimientos de protección de la información (PR.IP)	PR.IP-2	Se implementa un ciclo de vida de desarrollo del sistema para gestionar los sistemas.
3. DETECTAR	1. Anomalías y Eventos (DE.AE)	DE.AE-5	Se establecen umbrales de alerta de incidentes.
	2. Monitoreo Continuo de la Seguridad (DE.CM)	DE.CM-4	Se detecta el código malicioso.
	3. Procesos de Detección (DE.DP)	DE.DP-1	Los roles y los deberes de detección están bien definidos para asegurar la responsabilidad.
4. RESPONDER	1. Planificación de la Respuesta (RS.RP)	RS.RP-1	El plan de respuesta se ejecuta durante o después de un incidente.
	2. Comunicaciones (RS.CO)	RS.CO-2	Los incidentes se informan de acuerdo con los criterios establecidos.
	3. Análisis (RS.AN)	RS.AN-1	Se investigan las notificaciones de los sistemas de detección.
5. RECUPERAR	1. Planificación de la recuperación (RC.RP)	RC.RP-1	El plan de recuperación se ejecuta durante o después de un incidente de seguridad cibernética.
	2. Mejoras (RC.IM)	RC.IM-1	Los planes de recuperación incorporan las lecciones aprendidas.
	3. Comunicaciones (RC.CO)	RC.CO-2	La reputación se repara después de un incidente.

El Modelo Operacional del Programa del Sistema de Seguridad de la Información, tiene en el Marco de ciberseguridad NIST está definido la siguiente figura. Respecto de las métricas y el estado objetivo se describen en el Anexo 3 de este documento.

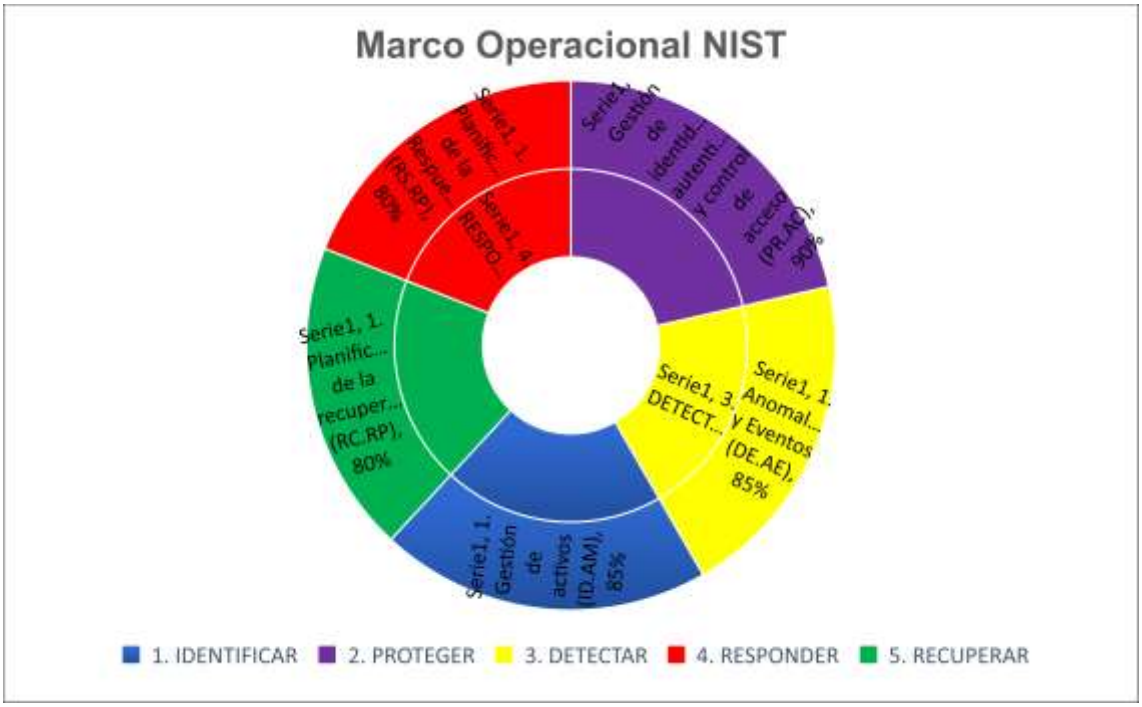


Figura 5. Marco Operacional NIST.

3.10. Programa del Sistema de Seguridad de la Información.

El programa del Sistema de Seguridad de la Información, se compone de los siguientes planes de acción, los mismos que son importantes para cubrir las brechas de seguridad identificadas en el diagnóstico inicial realizado en la empresa Grupo SES.

Tabla 16.

Planes de Acción

Planes de Acción	Código Plan de Acción	Dificultad	Valor	Orden de Implementación
Aprobar la política de seguridad de la información de acuerdo a las necesidades identificadas en la organización	**PLA.01**	Bajo	Bajo	1
Revisar de forma periódica las políticas de seguridad de la información para mantenerlas actualizadas	**PLA.02**	Bajo	Bajo	1

Establecer formalmente los roles y responsabilidades, conforme la política de seguridad establecida por la organización.	**PLA.03**	Bajo	Alto	1
Definir mediante una política el uso de dispositivos móviles, Smartphone, u otros dispositivos electrónicos sobre los que se puedan realizar intercambios de información.	**PLA.04**	Bajo	Alto	2
Proteger la información a la que se tiene acceso, que es procesada en lugares en los que se realiza teletrabajo.				
La organización debe mantener un inventario de recursos o activos de información.	**PLA.05**	Bajo	Alto	2
Los dueños de la información deben clasificar los niveles de sensibilidad de la misma, de acuerdo con la política de la seguridad de la información de la organización.				
Elaborar política de respaldos de la información considerada confidencial o sensible de la Organización.	**PLA.06**	Alto	Alto	2
Elaborar y aprobar la política de acceso para prevenir accesos no autorizados. Los privilegios sobre la información deben ser otorgados y mantenidos formalmente	**PLA.07**	Alto		
Establecer mecanismos de control de acceso físico y lógico para los usuarios	**PLA.08**	Alto		
Los empleados son responsables de sus acciones en el manejo de cualquier recurso de información de la organización.	**PLA.07**	Bajo	Bajo	3
El acceso a la información de la organización y de los sistemas, será de acuerdo con la política de control de acceso.				
Realizar estudios sobre la demanda y proyecciones de crecimiento de los recursos TI para establecer un plan de capacidades	**PLA.08**	Bajo	Bajo	3
Definir y aprobar la política de desarrollo seguro aplicando buenas prácticas y lineamientos de desarrollo seguro durante el ciclo de vida del software.				

Definir y aprobar la política de desarrollo seguro				
Elaborar y aprobar la política de gestión de incidentes de seguridad con el fin de prevenir y mitigar el impacto de los mismos.				
Analizar con todas las áreas involucradas la Implementación de los planes BCP y DRP.	**PLA.09**	Alto	Alto	4
Realizar una revisión independiente de la seguridad de la información por parte de un proveedor calificado.	**PLA.10**	Alto	Alto	4

Los planes de Acción del Sistema de Seguridad de la Información, tienen definidas métricas de evaluación y cronograma de ejecución para el año 2022, el cual está descrito en el Anexo 4.

4. CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

El Diagnóstico inicial sobre la seguridad de la información y los controles identificados, permitieron identificar y evaluar las amenazas y vulnerabilidades de los activos información críticos en la empresa.

El Diseño del Programa del Sistema de Seguridad de la Información propuesto, establece la aplicación de controles, mitigación de riesgos y políticas de alto nivel, para una mejor de gestión de la seguridad de la información en la empresa.

Las políticas de alto nivel, establecerán las directrices y los controles que se deben implementar, que permitan garantizar la confidencialidad, integridad y disponibilidad de la información, además minimizar los riesgos de seguridad.

El modelo de operación basado en el marco de ciberseguridad NIST, tiene como objetivo garantizar el funcionamiento del Sistema de Seguridad de la Información.

La ejecución de los planes de acción definidos permitirá a la empresa priorizar y alcanzar los objetivos de la seguridad de la información, y la respectiva alineación a los estándares, directrices y prácticas de ciberseguridad.

4.2 Recomendaciones

La implementación de los controles y procedimientos para asegurar los activos críticos de la información deben realizados conforme la evaluación realizada, por la Dirección de Tecnologías.

La ejecución del Programa del Sistema de Seguridad de la Información requiere del apoyo e involucramiento de la alta dirección, y así lograr el correcto funcionamiento del SGSI, mediante su evaluación y mejora continua.

Las políticas de alto nivel deben ser evaluadas y actualizadas, esto permitirá conocer el nivel cumplimiento de las directrices definidas en el Sistema de Seguridad de la Información.

Se debe asegurar y garantizar la operación Sistema de Gestión de Seguridad de la Información, en la empresa, para lo cual se debe evaluar conforme los parámetros establecidos por la Dirección de Tecnologías.

Los planes de acción son los más importantes dentro de la mejora del Sistema de Gestión de Seguridad de la Información, por lo tanto, se debe cumplir con su cronograma de implementación.

REFERENCIAS

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. (s.f.). Sistema de Gestión de Seguridad de la Información (SGSI). Recuperado el 2 de marzo de 2015 http://www.iso27000.es/sgsi.html

Consejo Superior de Administración Electrónica. (2012). Libro II Catálogo de Elementos. In C. S. Electrónica, MAGERIT V.3 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

ISACA. (2014). COBIT Focus Volumen 1. Recuperado el 5 de abril de 2016 de https://www.isaca.org/Knowledge-Center/cobit/cobit-focus/Pages/COBIT-Focus-Volumen-1-enero-de-2014.aspx

ISO. (2013). INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. Recuperado el 11 de marzo de 2016 de https://www.iso.org/ ISO/IEC. (2006). Técnicas de Seguridad, Sistemas de Gestión de la seguridad de la Información (SGSI) Requisitos (Primera ed.).

Sánchez Solá, Á. P. (2013). Diseño de un sistema de gestión de la seguridad de la información para comercio electrónico basado en la ISO 27001 para pequeñas y medianas empresas en la ciudad de Quito (Bachelor's thesis, QUITO/PUCE/2013).

Molano Espinel, R. A. (2017). Estrategia para implementar un sistema de gestión de la seguridad de la información basada en la norma ISO 27001 en el área de TI para la empresa Market Mix.

Enríquez Espinosa, P. R. Implementación de los controles asignados al dominio" Gestión de activos", bajo los lineamientos establecidos por la norma ISO/27001 Anexo A, para las empresas municipales de Cali, Emcali EICE-ESP.

Julio, A. Z., Joselin, P. G., & Martillo-Alchundia, I. EL ANÁLISIS Y GESTIÓN DE RIESGOS EN GOBIERNOS DE TI DESDE EL ENFOQUE DE LA METODOLOGÍA MAGERIT.

Gómez, E. F., Duchimaza, J., Holguín, J. R., & Lindao, M. A. (2019). Plan de contingencia para los equipos y sistemas informáticos utilizando la metodología MAGERIT. Revista Científica y Tecnológica UPSE, 6(1), 34-41.

Riesgo en la Seguridad de la Información. Ecuador. ISO27001.es. (2012). Sistema de Gestión de la Seguridad de la Información. Recuperado el 21 de marzo de 2016 de http://www.iso27000.es/download/doc_sgsi_all.pd.

ISOTools Excellence. (04 de agosto de 2014). Sitio web. ISO 27001 y la organización de la seguridad de la información en una PYME. https://www.pmg-ssi.com/2014/08/iso-27001-organizacion-seguridad-informacion-pyme/.

ISOTools Excellence. (2015). Blog especializado en Sistemas de Gestión de Seguridad de la Información. Recuperado el 11 de Abril de 2016 de http://www.pmg-ssi.com/2015/01/iso-27001-la-implementacion-de-un-sistema-de-gestion-de-seguridad-de-la-informacion

Instituto Nacional de Tecnologías de la Comunicación. (2014). Implantación de un SGSI en la empresa. Recuperado el 18 de Julio de 2016 de https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf.

ISO. (2013). International ORGANIZATION FOR STANDARDIZATION. Recuperado el 11 de marzo de 2016 de https://www.iso.org/

ISACA. (2012). COBIT 5 (Sexta ed.).

ISACA. (2014). COBIT Focus Volumen 1. Recuperado el 5 de Abril de 2016 de https://www.isaca.org/Knowledge-Center/cobit/cobit-focus/Pages/COBIT-Focus-Volumen-1-enero-de-2014.aspx

NIST Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 National Institute of Standards and Technology. Recuperado el 16

de abril de 2018 de https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Federal Trade Commission. (2021). Qué es y cómo funciona EL MARCO DE CIBERSEGURIDAD DEL NIST. Recuperado el 24 de agosto de 2021 de: https://www.ftc.gov/es/system/files/attachments/understanding-nist-cybersecurity-framework/cybersecurity_sb_nist-cyber-framework-es.pdf

Framework for Improving. Critical Infrastructure Cybersecurity. Version 1.1. National Institute of Standards and Technology. April 16, 2018.

Krumay, B., Bernroider, EW y Walser, R. (2018, noviembre). Evaluación de los controles y métricas de gestión de la ciberseguridad de las infraestructuras críticas: una revisión de la literatura considerando el Marco de Ciberseguridad del NIST. En la Conferencia nórdica sobre sistemas informáticos seguros (págs. 369-384). Springer, Cham.

ANEXOS

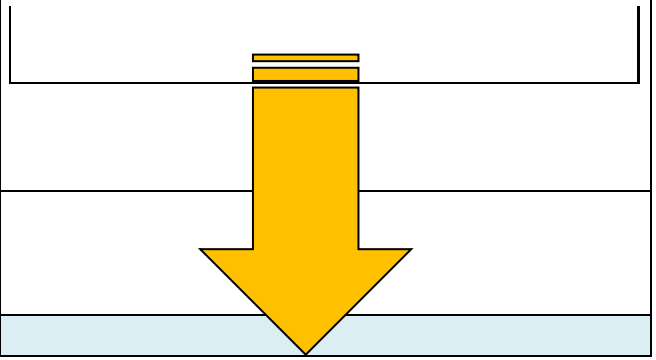
Anexo 1

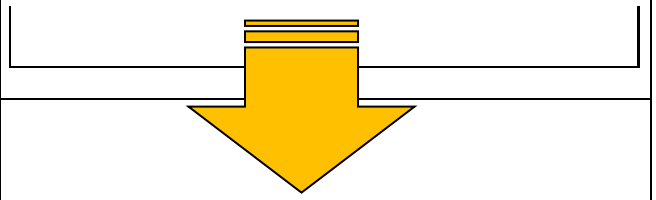
ANÁLISIS DEL CONTEXTO DE LA ORGANIZACIÓN DIAGNOSTICO ISO 27001							
Sección	**Requerimientos ISO 27001**	**Estado Actual**	**Porcentaje Actual**	**Estado Objetivo**	**Porcentaje Objetivo**	**Responsable**	**Acciones de Mejora**
4	**Contexto de la organización**						
4.1	**Comprensión de la organización y de su contexto**						
4.1	Determinar los objetivos del SGSI de la organización y cualquier problema que pueda afectar su eficacia	Inicial	10	Administrado	95	Director de Tecnologías	La organización debe identificar las partes interesadas y los requisitos que son relevantes para el sistema de gestión de seguridad de la información.
4.2	**Comprensión de las necesidades y expectativas de las partes interesadas**						
4.2 (a)	Identificar las partes interesadas incluyendo leyes aplicables,	Inicial	10	Administrado	95	Director de Tecnologías	Determinar los objetivos en la seguridad de la información en relación directa con los propios objetivos de la organización

	regulaciones, contratos, etc.						
4.2 (b)	Determinar los requerimientos y obligaciones relevantes de seguridad de la información	Inicial	10	Administrado	95	Director de Tecnologías	
4.3	**Determinación del alcance del SGSI**						
4.3	Determinar y documentar el alcance del SGSI	Inicial	10	Administrado	95	Director de Tecnologías	
4.4	**SGSI**						
4.4	Establecer, implementar, mantener y mejorar de forma continua el SGSI acorde al estándar	Inicial	10	Administrado	95	Coordinador de Proyectos TI	
5	**Liderazgo**						
5.1	**Liderazgo y compromiso**						
5.1	La administración debe demostrar liderazgo y compromiso por el SGSI	Definido	90	Administrado	95	Director de Tecnologías	Aplicación de la política de seguridad y establecer los objetivos de la seguridad de la información
5.2	**Política**						

5.2	Documentar la Política de Seguridad de la Información	Definido	90	Administrado	95	Coordinador de Proyectos TI	Aprobación de la política de seguridad de la Información
5.3	**Roles, responsabilidades y autoridades en la organización**						
5.3	Asignar y comunicar los roles y responsabilidades de seguridad de la información	Definido	90	Administrado	95	Coordinador de Desarrollo TI	Definir las áreas de responsabilidad y los roles correspondientes a la seguridad de la información
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	Inicial	10	Definido	90	Coordinador de Seguridad TI	Establecer un plan para definir los riesgos que se debe tratar con las actividades a realizar para mitigar los riesgos
6.1.2	Definir e implementar un proceso de análisis de riesgos de seguridad de la información	Inicial	10	Definido	90	Coordinador de Seguridad TI	

6.1.3	Documentar e implementar un proceso de tratamiento de riesgos de seguridad de la información	Inicial	10	Definido	90	Coordinador de Seguridad TI	
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	10	Definido	90	Coordinador de Proyectos TI	
7	**Soporte**						
7.1	**Recursos**						
7.1	Determinar y asignar los recursos necesarios para el SGSI	Inicial	10	Definido	90	Coordinador de Proyectos TI	Establecer los proyectos y la inversión inicial acorde con la evaluación de riesgos y los criterios para minimizar los riesgos
7.2	**Competencia**						
7.2	Determinar, documentar hacer disponibles las competencias necesarias	Inicial	10	Definido	90	Coordinador de Proyectos TI	Fortalecer la competencia del personal de TICS

7.3	**Concienciación**						
7.3	Implementar un programa de concientización de seguridad	Inicial	10	Definido	90	Coordinador de Seguridad TI	Implantar una cultura de la seguridad dentro de su organización
7.4	**Comunicación**						
7.4	Determinar la necesidades de comunicación internas y externas relacionadas al SGSI	Inicial	10	Definido	90	Coordinador de Seguridad TI	Comunicar los objetivos a toda la organización con el objeto de involucrar a todos los empleados con los objetivos de la seguridad de la información
7.5	**Información documentada**						
7.5.1	Proveer documentación requerida por el estándar más la requerida por la organización	Inicial	10	Definido	90	Coordinador de Proyectos TI	Elaborar, aprobar y documentar los procesos internos relacionados con la seguridad de la información
7.5.2	Proveer un título, autor, formato consistente, revisión y aprobación a los documentos	Inicial	10	Definido	90	Coordinador de Proyectos TI	
7.5.3	Mantener un control adecuado de la documentación	Inicial	10	Definido	90	Coordinador de Proyectos TI	
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)	Inicial	10	Definido	90	Coordinador de Proyectos TI	Ejecutar el seguimiento y supervisión del plan de tratamiento de riesgos y su integración en los procesos de la organización
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	10	Definido	90	Coordinador de Seguridad TI	
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	10	Definido	90	Coordinador de Seguridad TI	
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	10	Definido	90	Coordinador de Seguridad TI	Establecer indicadores de medición para garantizar la correcta operación del SGSI como parte de la mejora continua.
9.2	**Auditoría interna**						
9.3	Planificar y realizar una auditoria interna del SGSI	Inicial	10	Definido	90	Coordinador de Seguridad TI	Planificar una auditoria inicial interna del SGSI
9.3	**Revisión por la dirección**						
9.3	La administración realiza una revisión periódica del SGSI	Inicial	10	Definido	90	Coordinador de Seguridad TI	Definir y aprobar la revisión periódica del SGSI por la alta dirección.
10	**Mejora**						
10.1	**No conformidad y acciones correctivas**						
10.1	Identificar, arreglar y reaccionar ante no conformidades	Inicial	10	Definido	90	Coordinador de Seguridad TI	Revisión de cumplimientos normativos o sobre procesos internos propios de la organización

	para evitar su recurrencia documentando todas las acciones						
10.2	**Mejora continua**						
10.2	Mejora continua del SGSI	Inicial	10	Definido	90	Coordinador de Seguridad TI	Monitoreo de KPIs

Anexo 2

Sección	Controles de Seguridad de la Información	Estado Actual	Porcentaje Actual	Estado Objetivo	Porcentaje Objetivo	Responsable	Planes de Acción	Código Plan de Acción
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	Definido	90	Administrado	95	Director de Tecnologías	Aprobar la política de seguridad de la información de acuerdo a las necesidades identificadas en la organización	**PLA. 01**
A5.1.2	Revisión de las políticas para la seguridad de la información	Definido	90	Administrado	95	Director de Tecnologías	Revisar de forma periódica las políticas de seguridad de la información para mantenerlas actualizadas	**PLA. 02**
A6	**Organización de la seguridad de la información**							
A6.1	**Organización interna**							

A6.1.1	Roles y responsabilidades en seguridad de la información	Repetible	50	Administrado	95	Coordinador de Seguridad TI	Establecer formalmente los roles y responsabilidades, conforme la política de seguridad establecida por la organización.	**PLA. 03**
A6.1.2	Segregación de tareas	Definido	90	Administrado	95	Coordinador de Seguridad TI		
A6.1.3	Contacto con las autoridades	Repetible	50	Administrado	95	Coordinador de Seguridad TI		
A6.1.4	Contacto con grupos de interés especial	Definido	90	Administrado	95	Coordinador de Seguridad TI		
A6.1.5	Seguridad de la información en la gestión de proyectos	Repetible	50	Administrado	95	Coordinador de Seguridad TI	En la planeación y ejecución de los proyectos debe participar el área de Seguridad de la Información como generador de recomendaciones en la evaluación de	

							los riesgos inherentes	
A6.2	**Los dispositivos móviles y el teletrabajo**							
A6.2.1	Política de dispositivos móviles	Repetible	50	Administrado	95	Coordinador de Seguridad TI	Definir mediante una política el uso de dispositivos móviles, Smartphone, u otros dispositivos electrónicos sobre los que se puedan realizar intercambios de información.	**PLA. 04**
A6.2.2	Teletrabajo	Repetible	50	Administrado	95	Coordinador de Seguridad TI	Proteger la información a la que se tiene acceso, que es procesada en lugares en los que se realiza teletrabajo.	
A7	**Seguridad relativa a los recursos humanos**							
A7.1	**Antes del empleo**							
A7.1.1	Investigación de antecedentes	Definido	90	Administrado	95	Responsable de	Proceso de investigación de	

						Talento Humano	antecedentes, con el fin de mitigar los riesgos en el uso de la información	
A7.1.2	Términos y condiciones del empleo	Definido	90	Administrado	95	Responsable de Talento Humano	Los contratos de los empleados deben incluir cláusulas que especifiquen las responsabilidades y los cuidados que deben tener con la información de la Organización.	
A7.2	**Durante el empleo**							
A7.2.1	Responsabilidades de gestión	Definido	90	Administrado	95	Responsable de Talento Humano	La organización debe proveer los mecanismos necesarios para asegurar que sus empleados cumplan con sus responsabilidades	

A7.2.2	Concienciación, educación y capacitación en seguridad de la información	Repetible	50	Administrado	95	Responsable de Talento Humano	La organización debe establecer un programa permanente de creación de cultura en seguridad de la información para los empleados y terceros	
A7.2.3	Proceso disciplinario	Definido	90	Administrado	95	Responsable de Talento Humano	La Política de Seguridad de la Información, procedimientos que soportan el Sistema de Gestión de Seguridad de la Información son de cumplimiento obligatorio.	
A7.3	**Finalización del empleo o cambio en el puesto de trabajo**							
A7.3.1	Responsabilidades ante la finalización o cambio	Definido	90	Administrado	95	Responsable de Talento Humano	Informar a los empleados o contratistas, las responsabilidades en la entrega de la información después de la	

							terminación o cambio de contrato.	
A8	**Gestión de activos**							
A8.1	**Responsabilidad sobre los activos**							
A8.1.1	Inventario de activos	Repetible	50	Administrado	95	Coordinador de Infraestructura TI	La organización debe mantener un inventario de recursos o activos de información.	**PLA. 05**
A8.1.2	Propiedad de los activos	Definido	90	Administrado	95	Coordinador de Infraestructura TI		
A8.1.3	Uso aceptable de los activos	Definido	90	Administrado	95	Coordinador de Infraestructura TI		
A8.1.4	Devolución de activos	Definido	90	Administrado	95	Coordinador de Infraestructura TI		
A8.2	**Clasificación de la información**							
A8.2.1	Clasificación de la información	Repetible	50	Administrado	95	Coordinador de Seguridad TI	Los dueños de la información deben clasificar los niveles de sensibilidad de la misma, de acuerdo con la política de la	

							seguridad de la información de la organización.	
A8.2.2	Etiquetado de la información	Repetible	50	Administrado	95	Coordinador de Seguridad TI		
A8.2.3	Manipulado de la información	Repetible	50	Administrado	95	Coordinador de Seguridad TI		
A8.3	**Manipulación de los soportes**							
A8.3.1	Gestión de soportes extraíbles	Repetible	50	Administrado	95	Coordinador de Infraestructura TI	No está permitido la conexión a la red de la Organización de equipos portátiles, computadores, dispositivos móviles o cualquier otro dispositivo, de uso personal de los empleados, sin autorización del Director de Tics.	
A8.3.2	Eliminación de soportes	Repetible	50	Administrado	95	Coordinador de Infraestructura TI	Elaborar política de respaldos de la información	**PLA. 06**

							considerada confidencial o sensible de la Organización.	
A8.3.3	Soportes físicos en tránsito	Repetible	50	Administrado	95	Coordinador de Infraestructura TI	Los equipos tecnológicos que contengan información deben estar protegidos contra accesos no autorizados, usos indebidos o deterioro	
A9	**Control de acceso**							
A9.1	**Requisitos de negocio para el control de acceso**							
A9.1.1	Política de control de acceso	Inicial	10	Administrado	95	Coordinador de Seguridad TI	Elaborar y aprobar la política de acceso para prevenir accesos no autorizados. Los privilegios sobre la información deben ser otorgados y mantenidos formalmente	**PLA. 07**
A9.1.2	Acceso a las redes y a los servicios de red	Inicial	10	Administrado	95	Coordinador de	el acceso a la red de es solo a usuarios	

						Seguridad TI	autorizados por el Director de Tics.	
A9.2	**Gestión de acceso de usuario**							
A9.2.1	Registro y baja de usuario	Repetible	50	Administrado	95	Coordinador de Seguridad TI	Establecer los procedimientos para el registro, baja y del acceso de los usuarios a los sistemas conforme la política de seguridad	
A9.2.2	Provisión de acceso de usuario	Repetible	50	Administrado	95	Coordinador de Seguridad TI	Establecer mecanismos de control de acceso físico y lógico para los usuarios	**PLA. 08**
A9.2.3	Gestión de privilegios de acceso	Inicial	10	Administrado	95	Coordinador de Seguridad TI	Restringir el acceso a información que se considere inconveniente para la organización	
A9.2.4	Gestión de la información secreta de autenticación de los usuarios	Inicial	10	Administrado	95	Coordinador de Seguridad TI	El acceso restringido se aplica únicamente a los sistemas críticos de la organización	

A9.2.5	Revisión de los derechos de acceso de usuario	Inicial	10	Administrado	95	Coordinador de Seguridad TI	Aplicar un sistema de identificación y el acceso debe ser controlado a través de una autenticación cifrada.	
A9.2.6	Retirada o reasignación de los derechos de acceso	Inicial	10	Administrado	95	Coordinador de Seguridad TI	Este control se realiza en la actualidad de forma individual.	
A9.3	**Responsabilidades del usuario**							
A9.3.1	Uso de la información secreta de autenticación	Definido	90	Administrado	95	Coordinador de Seguridad TI	Los empleados son responsables de sus acciones en el manejo de cualquier recurso de información de la organización.	**PLA. 07**
A9.4	**Control de acceso a sistemas y aplicaciones**							
A9.4.1	Restricción del acceso a la información	Definido	90	Administrado	95	Coordinador de Seguridad TI	El acceso a la información de la organización y de los sistemas, será de acuerdo con la política	**PLA. 07**

							de control de acceso.	
A9.4.2	Procedimientos seguros de inicio de sesión	Definido	90	Administrado	95	Coordinador de Seguridad TI	Controlar que los usuarios sigan buenas prácticas de seguridad para protección de contraseñas.	
A9.4.3	Sistema de gestión de contraseñas	Repetible	50	Administrado	95	Coordinador de Seguridad TI	La política de seguridad establece los lineamientos en la definición de contraseñas.	
A9.4.4	Uso de utilidades con privilegios del sistema	Repetible	50	Administrado	95	Coordinador de Seguridad TI	Este control se encuentra implementado en el área de TICS	
A9.4.5	Control de acceso al código fuente de los programas	Repetible	50	Administrado	95	Coordinador de Seguridad TI	El área de TICS es quien tiene acceso al código fuente	
A10	**Criptografía**							
A10.1	**Controles criptográficos**							
A10.1.1	Política de uso de los controles criptográficos	Repetible	50	Administrado	95	Coordinador de Seguridad TI	La información restringida, es cifrada al	

							momento de almacenarse	
A10.1.2	Gestión de claves	Repetible	50	Administrado	95	Coordinador de Seguridad TI	Este control se encuentra implementado en el área de TICS	
A11	**Seguridad física y del entorno**							
A11.1	**Áreas seguras**							
A11.1.1	Perímetro de seguridad física	Definido	90	Administrado	95	Coordinador de Seguridad TI	Actualmente cada una de las áreas cuenta con el espacio definido.	
A11.1.2	Controles físicos de entrada	Definido	90	Administrado	95	Coordinador de Seguridad TI	Actualmente cada una de las áreas cuenta con acceso a cada uno de sus empleados	
A11.1.3	Seguridad de oficinas, despachos y recursos	Definido	90	Administrado	95	Coordinador de Seguridad TI	Actualmente cada una de las áreas cuenta con acceso independiente	
A11.1.4	Protección contra las amenazas externas y ambientales	Definido	90	Administrado	95	Coordinador de	Las condiciones físicas y	

						Seguridad TI	ambientales son las necesarias para trabajar adecuadamente	
A11.1.5	El trabajo en áreas seguras	Definido	90	Administrado	95	Coordinador de Seguridad TI	Cuenta con mecanismos de seguridad física y control de acceso	
A11.1.6	Áreas de carga y descarga	Inexistente	0	Inexistente	0	**N/A**	**No Aplica**	
A11.2	**Seguridad de los equipos**							
A11.2.1	Emplazamiento y protección de equipos	Definido	90	Administrado	95	Coordinador de Seguridad TI	Los recursos informáticos están físicamente protegidos	
A11.2.2	Instalaciones de suministro	Definido	90	Administrado	95	Coordinador de Seguridad TI	Existen contratos de mantenimiento y soporte técnico vigentes	
A11.2.3	Seguridad del cableado	Definido	90	Administrado	95	Coordinador de Seguridad TI	El cableado estructurado está certificado y garantía vigente	
A11.2.4	Mantenimiento de los equipos	Definido	90	Administrado	95	Coordinador de Seguridad TI	Existen contratos de mantenimiento y soporte	

							técnico vigentes	
A11.2.5	Retirada de materiales propiedad de la empresa	Inexistente	0	Inexistente	0	**N/A**	**No Aplica**	
A11.2.6	Seguridad de los equipos fuera de las instalaciones	Repetible	50	Definido	90	Coordinador de Infraestructura TI	Existe control de los equipos que están fuera de las instalaciones	
A11.2.7	Reutilización o eliminación segura de equipos	Inicial	10	Definido	90	Coordinador de Infraestructura TI	El área de Tecnología debe efectuar la reutilización o retirada segura de los equipos informáticos.	
A11.2.8	Equipo de usuario desatendido	Repetible	50	Definido	90	Coordinador de Seguridad TI	El trabajo mediante acceso remoto, se cuenta con controles de acceso definidos.	
A11.2.9	Política de puesto de trabajo despejado y pantalla limpia	Inicial	10	Definido	90	Coordinador de Seguridad TI	Los empleados son responsables de sus acciones en el manejo de cualquier recurso de información de la organización.	

A12	**Seguridad de las operaciones**							
A12.1	**Procedimientos y responsabilidades operacionales**							
A12.1.1	Documentación de procedimientos operacionales	Inicial	10	Definido	90	Coordinador de Desarrollo TI	El área de tecnología en la actualidad no tiene documentada toda la información relacionada con la administración de los sistemas.	
A12.1.2	Gestión de cambios	Inicial	10	Definido	90	Coordinador de Desarrollo TI	Establecer un procedimiento control de cambios	
A12.1.3	Gestión de capacidades	Inicial	10	Definido	90	Coordinador de Desarrollo TI	Realizar estudios sobre la demanda y proyecciones de crecimiento de los recursos TI para establecer un plan de capacidades	**PLA. 08**
A12.1.4	Separación de los recursos de desarrollo, prueba y operación	Definido	90	Administrado	95	Coordinador de Desarrollo TI	Existen ambientes de prueba y desarrollo de acuerdo a la	

							necesidad de la organización	
A12.2	**Protección contra el software malicioso (malware)**							
A12.2.1	Controles contra el código malicioso	Definido	90	Administrado	95	Coordinador de Seguridad TI	La protección de la información y los recursos de la plataforma tecnológica es mediante software especializado	
A12.3	**Copias de seguridad**							
A12.3.1	Copias de seguridad de la información	Definido	90	Administrado	95	Coordinador de Seguridad TI	Las copias de seguridad siempre son realizadas por TICS.	**PLA. 06**
A12.4	**Registros y supervisión**							
A12.4.1	Registro de eventos	Definido	90	Administrado	95	Coordinador de Infraestructura TI	TICS tiene pantallas de monitoreo que permite identificar eventos en sus sistemas.	
A12.4.2	Protección de la información del registro	Definido	90	Administrado	95	Coordinador de Infraestructura TI	TICS es responsable de la integridad y disponibilidad de los registros de auditoria	

							generados en los sistemas informáticos	
A12.4.3	Registros de administración y operación	Definido	90	Administrado	95	Coordinador de Infraestructura TI	TICS realiza monitoreo de los eventos en los sistemas, con el fin de evitar accesos no autorizados de información	
A12.4.4	Sincronización del reloj	Definido	90	Administrado	95	Coordinador de Infraestructura TI	TICS es responsable de la sincronización	
A12.5	**Control del software en explotación**							
A12.5.1	Instalación del software en explotación	Inicial	10	Definido	90	Coordinador de Desarrollo TI	TICS designa responsables para controlar la instalación de software operativo	
A12.6	**Gestión de la vulnerabilidad técnica**							
A12.6.1	Gestión de las vulnerabilidades técnicas	Repetible	50	Administrado	95	Coordinador de Desarrollo TI	El responsable de Desarrollo es quien valida este control	
A12.6.2	Restricción en la instalación de software	Repetible	50	Administrado	95	Coordinador de Desarrollo TI	El responsable de Desarrollo es quien valida este control	
A12.7	**Consideraciones sobre la auditoria de sistemas de información**							

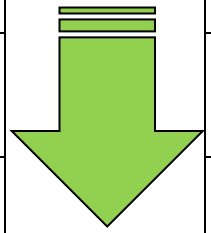
A12.7.1	Controles de auditoría de sistemas de información	Inicial	10	Definido	90	Coordinador de Seguridad TI	Se realiza monitoreo de los eventos	
A13	**Seguridad de las comunicaciones**							
A13.1	**Gestión de la seguridad de las redes**							
A13.1.1	Controles de red	Definido	90	Administrado	95	Coordinador de Infraestructura TI	Las redes de datos y de los servicios que dependientes son administrados por TICS.	
A13.1.2	Seguridad de los servicios de red	Definido	90	Administrado	95	Coordinador de Infraestructura TI	Las redes de datos y de los servicios que dependientes son administrados por TICS.	
A13.1.3	Segregación en redes	Definido	90	Administrado	95	Coordinador de Infraestructura TI	Las redes de datos y de los servicios que dependientes son administrados por TICS.	
A13.2	**Intercambio de información**							
A13.2.1	Políticas y procedimientos de intercambio de información	Definido	90	Administrado	95	Coordinador de Seguridad TI	La información que se envía es por correo seguro y cifrada para	

							evitar fugas de información.	
A13.2.2	Acuerdos de intercambio de información	Definido	90	Administrado	95	Coordinador de Seguridad TI	Existen Acuerdos de Confidencialidad.	
A13.2.3	Mensajería electrónica	Definido	90	Administrado	95	Coordinador de Seguridad TI	El correo electrónico es un servicio seguro para la ejecución de las actividades.	
A13.2.4	Acuerdos de confidencialidad o no revelación	Definido	90	Administrado	95	Coordinador de Seguridad TI	Existen Acuerdos de Confidencialidad.	
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	Repetible	50	Administrado	95	Coordinador de Seguridad TI	Los requerimientos de seguridad de la información son definidos en los sistemas de información.	
A14.1.2	Asegurar los servicios de aplicaciones en redes públicas	Repetible	50	Administrado	95	Coordinador de Seguridad TI	Se aplican controles de seguridad	

							mediante cifrado	
A14.1.3	Protección de las transacciones de servicios de aplicaciones	Repetible	50	Administrado	95	Coordinador de Seguridad TI	Se aplican controles de seguridad mediante cifrado	
A14.2	**Seguridad en el desarrollo y en los procesos de soporte**							
A14.2.1	Política de desarrollo seguro	Inicial	10	Administrado	95	Coordinador de Desarrollo TI	Definir y aprobar la política de desarrollo seguro aplicando buenas prácticas y lineamientos de desarrollo seguro durante el ciclo de vida del software.	**PLA. 08**
A14.2.2	Procedimiento de control de cambios en sistemas	Inicial	10	Administrado	95	Coordinador de Desarrollo TI		
A14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	Inicial	10	Administrado	95	Coordinador de Desarrollo TI		
A14.2.4	Restricciones a los cambios en los paquetes de software	Inicial	10	Administrado	95	Coordinador de Desarrollo TI		

A14.2.5	Principios de ingeniería de sistemas seguros	Inicial	10	Administrado	95	Coordinador de Desarrollo TI		
A14.2.6	Entorno de desarrollo seguro	Inicial	10	Administrado	95	Coordinador de Desarrollo TI		
A14.2.7	Externalización del desarrollo de software	Inicial	10	Administrado	95	Coordinador de Desarrollo TI		
A14.2.8	Pruebas funcionales de seguridad de sistemas	Inicial	10	Administrado	95	Coordinador de Desarrollo TI		
A14.2.9	Pruebas de aceptación de sistemas	Inicial	10	Administrado	95	Coordinador de Desarrollo TI		
A14.3	**Datos de prueba**							
A14.3.1	Protección de los datos de prueba	Inicial	10	Administrado	95	Coordinador de Desarrollo TI	Definir y aprobar la política de desarrollo seguro	**PLA. 08**
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	Definido	90	Administrado	95	Coordinador de Seguridad TI	Existen Acuerdos de Confidencialidad.	

A15.1.2	Requisitos de seguridad en contratos con terceros	Definido	90	Administrado	95	Coordinador de Seguridad TI	Existen Acuerdos de Confidencialidad.	
A15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	Definido	90	Administrado	95	Coordinador de Seguridad TI	Existen Acuerdos de Confidencialidad.	
A15.2	**Gestión de la provisión de servicios del proveedor**							
A15.2.1	Control y revisión de la provisión de servicios del proveedor	Definido	90	Administrado	95	Coordinador de Seguridad TI	Existen Acuerdos de SLA vigentes.	
A15.2.2	Gestión de cambios en la provisión del servicio del proveedor	Definido	90	Administrado	95	Coordinador de Seguridad TI	Existen Acuerdos de SLA vigentes.	
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	50	Administrado	95	Coordinador de Seguridad TI	Elaborar y aprobar la política de gestión de incidentes de seguridad con el fin de prevenir y mitigar el impacto de los mismos.	**PLA. 08**

A16.1.2	Notificación de los eventos de seguridad de la información	Repetible	50	Administrado	95	Coordinador de Seguridad TI		
A16.1.3	Notificación de puntos débiles de la seguridad	Repetible	50	Administrado	95	Coordinador de Seguridad TI		
A16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	Repetible	50	Administrado	95	Coordinador de Seguridad TI		
A16.1.5	Respuesta a incidentes de seguridad de la información	Repetible	50	Administrado	95	Coordinador de Seguridad TI		
A16.1.6	Aprendizaje de los incidentes de seguridad de la información	Repetible	50	Administrado	95	Coordinador de Seguridad TI		
A16.1.7	Recopilación de evidencias	Inicial	10	Definido	90	Coordinador de Seguridad TI		
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	Inicial	10	Administrado	95	Coordinador de Seguridad TI	Implementar y verificar periódicamente procedimientos que se aseguren la	

							recuperación de la información sensible de la organización.	
A17.1.2	Implementar la continuidad de la seguridad de la información	Inicial	10	Administrado	95	Coordinador de Seguridad TI	Establecer procesos de contingencia.	
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Inicial	10	Administrado	95	Coordinador de Seguridad TI	Analizar con todas las áreas involucradas la Implementación de los planes BCP y DRP.	**PLA. 09**
A17.2	**Redundancias**							
A17.2.1	Disponibilidad de los recursos de tratamiento de la información	Inicial	10	Administrado	95	Coordinador de Infraestructura TI	Contrato de AWS de Amazon vigente	
A18	**Cumplimiento**							
A18.1	**Cumplimiento de los requisitos legales y contractuales**							
A18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Definido	90	Administrado	95	Asesor Legal	Aplicación de la normatividad vigente en el país.	
A18.1.2	Derechos de Propiedad Intelectual (DPI)	Definido	90	Administrado	95	Asesor Legal	Aplicación de la normatividad vigente en el país.	
A18.1.3	Protección de los registros de la organización	Definido	90	Administrado	95	Director de Tecnologías	TICS realiza el monitoreo de	

							las aplicaciones	
A18.1.4	Protección y privacidad de la información de carácter personal	Definido	90	Administrado	95	Director de Tecnologías	TICS realiza el monitoreo de las aplicaciones	
A18.1.5	Regulación de los controles criptográficos	Repetible	50	Administrado	95	Director de Tecnologías	Los controles criptográficos para proteger la información están definidos.	
A18.2	**Revisiones de la seguridad de la información**							
A18.2.1	Revisión independiente de la seguridad de la información	Inicial	10	Definido	90	Director de Tecnologías	Realizar una revisión independiente de la seguridad de la información por parte de un proveedor calificado.	**PLA. 10**
A18.2.2	Cumplimiento de las políticas y normas de seguridad	Inicial	10	Definido	90	Director de Tecnologías	Definir las procedimientos de verificación de seguridad de la información.	
A18.2.3	Comprobación del cumplimiento técnico	Inicial	10	Definido	90	Director de Tecnologías	Validación de los controles técnicos de seguridad TI	

Anexo 3.

MODELO OPERACIONAL NIST Y MÉTRICAS

Función	Categoría	Subcategoría	Descripción Subcategoría	Métricas	Evaluación Métrica	Indicadores			Estado Objetivo
						B	M	A	
1. IDENTIFICAR	1. Gestión de activos (ID.AM)	ID.AM-1	Los dispositivos y sistemas físicos dentro de la organización están inventariados.	Número de activos no autorizados identificados	Trimestral			85%	85%
	3. Gobernanza (ID.GV)	ID.GV-1	Se establece y se comunica la política de seguridad cibernética organizacional.	Porcentaje de personas que demuestran una mejora en la medición comportamientos de seguridad de la información	Semestral			85%	
	4. Evaluación de riesgos (ID.RA)	ID.RA-1	Se identifican y se documentan las vulnerabilidades de los activos.	Número de incidentes con calificaciones de riesgo debidamente designadas	Semestral			85%	
2. PROTEGER	1. Gestión de identidad, autenticación y control de acceso (PR.AC)	PR.AC-1	Las identidades y credenciales se emiten, se administran, se verifican, se revocan y se	Porcentaje de sistemas administrados con identidad y acceso automatizados	Trimestral			90%	90%

			auditan para los dispositivos, usuarios y procesos autorizados.						
	2. Concienciación y capacitación (PR.AT)	PR.AT-1	Todos los usuarios están informados y capacitados.	Porcentaje de usuarios que han completado un programa de concientización sobre seguridad de la información	Semestral			90%	
	4. Procesos y procedimientos de protección de la información (PR.IP)	PR.IP-2	Se implementa un ciclo de vida de desarrollo del sistema para gestionar los sistemas.	Número de soluciones revisadas debido a la falta de requisitos de seguridad de la información	Semestral			90%	
3. DETECTAR	1. Anomalías y Eventos (DE.AE)	DE.AE-5	Se establecen umbrales de alerta de incidentes.	Porcentaje de riesgo de TI mitigado	Semestral			85%	85%
	2. Monitoreo Continuo de la Seguridad (DE.CM)	DE.CM-4	Se detecta el código malicioso.	Porcentaje de falsos positivos descubiertos durante monitoreo de seguridad de la información	Trimestral			90%	
	3. Procesos de Detección (DE.DP)	DE.DP-1	Los roles y los deberes de detección están bien definidos para asegurar la responsabilidad.	Número de roles con responsabilidades definidas en la gestión de Sistemas	Anual		80%		

4. RESPONDER	1. Planificación de la Respuesta (RS.RP)	RS.RP-1	El plan de respuesta se ejecuta durante o después de un incidente.	Porcentaje de riesgo de TI mitigado	Anual		80%		80%
	2. Comunicaciones (RS.CO)	RS.CO-2	Los incidentes se informan de acuerdo con los criterios establecidos.	Porcentaje de eventos descubiertos durante el monitoreo de la seguridad de la información	Semestral		80%		
	3. Análisis (RS.AN)	RS.AN-1	Se investigan las notificaciones de los sistemas de detección.	Porcentaje de falsos positivos identificados a partir de la información incidentes de seguridad	Semestral		80%		
5. RECUPERAR	1. Planificación de la recuperación (RC.RP)	RC.RP-1	El plan de recuperación se ejecuta durante o después de un incidente de seguridad cibernética.	Porcentaje de incidentes que requieren cambios de configuración o procedimientos	Anual		80%		80%
	2. Mejoras (RC.IM)	RC.IM-1	Los planes de recuperación incorporan las lecciones aprendidas.	Porcentaje de riesgo de TI mitigado	Anual		80%		
	3. Comunicaciones (RC.CO)	RC.CO-2	La reputación se repara después de un incidente.	Porcentaje de riesgo de TI mitigado	Semestral		80%		

Anexo 4.

Planes de Acción	Código Plan de Acción	Dificultad	Valor	Orden de Implementación	Métricas	Costo	Año 2022			
							Primer Trimestre	Segundo Trimestre	Tercer Trimestre	Cuarto Trimestre
Aprobar la política de seguridad de la información de acuerdo a las necesidades identificadas en la organización	**PLA.01**	Bajo	Bajo	1	% de total requerido de políticas, procedimientos de concientización y capacitación que se han desarrollado.	Salario del Responsable				
Revisar de forma periódica las políticas de seguridad de la información para mantenerlas actualizadas	**PLA.02**	Bajo	Bajo	1	% cambios o actualización de la política.	Salario del Responsable				
Establecer formalmente los roles y responsabilidades, conforme la política de seguridad	**PLA.03**	Bajo	Alto	1	% de roles y perfiles asignados para el acceso a información organizacional y de los sistemas de información.	Salario del Responsable				

establecida por la organización.										
Definir mediante una política el uso de dispositivos móviles, Smartphone, u otros dispositivos electrónicos sobre los que se puedan realizar intercambios de información.	**PLA.04**	Bajo	Alto	2	% de dispositivos controlados y autorizados para acceder a los sistemas y servicios informáticos de la organización.	Salario del Responsable				
Proteger la información a la que se tiene acceso, que es procesada en lugares en los que se realiza teletrabajo.										
La organización debe mantener un inventario de recursos o activos de información.	**PLA.05**	Bajo	Alto	2	% de activos informáticos registrados e inventariados.	Salario del Responsable				

Los dueños de la información deben clasificar los niveles de sensibilidad de la misma, de acuerdo con la política de la seguridad de la información de la organización.										
Elaborar política de respaldos de la información considerada confidencial o sensible de la Organización.	**PLA.06**	Alto	Alto	2	% de respaldos generados. % de permisos asignados a recursos de información. % de controles implementados.	Salario del Responsable				
Elaborar y aprobar la política de acceso para prevenir accesos no autorizados. Los privilegios sobre la información deben ser otorgados y mantenidos formalmente	**PLA.07**	Alto								
Establecer mecanismos de control de acceso físico y	**PLA.08**	Alto								

lógico para los usuarios										
Los empleados son responsables de sus acciones en el manejo de cualquier recurso de información de la organización.	**PLA.07**	Bajo	Bajo	3	% de acciones adecuadas al tratamiento y uso de la información.	Salario del Responsable				
El acceso a la información de la organización y de los sistemas, será de acuerdo con la política de control de acceso.										
Realizar estudios sobre la demanda y proyecciones de crecimiento de los recursos TI para establecer un plan de capacidades	**PLA.08**	Bajo	Bajo	3	% de infraestructura TI disponible	Salario del Responsable				
Definir y aprobar la política de desarrollo seguro aplicando					% de aplicaciones que cumplen con el desarrollo seguro					

buenas prácticas y lineamientos de desarrollo seguro durante el ciclo de vida del software.										
Definir y aprobar la política de desarrollo seguro					% de aplicación de la política de desarrollo seguro					
Elaborar y aprobar la política de gestión de incidentes de seguridad con el fin de prevenir y mitigar el impacto de los mismos.					% de aplicación de políticas de incidentes					
Analizar con todas las áreas involucradas la Implementación de los planes BCP y DRP.	**PLA.09**	Alto	Alto	4	% de avance del alcance BCP % de avance del DRP	Salario del Responsable				
Realizar una revisión independiente de la seguridad de la información por parte de un	**PLA.10**	Alto	Alto	4	% de auditorías externas revisadas	Salario del Responsable				

proveedor calificado.										