FACULTAD DE POSGRADO

PROPUESTA DEL PROGRAMA DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION PARA EL PROCESO DE GESTION DE TI DE TRANSPORTES SEGUROS S.A.

Carlos Guillermo Vargas Álvarez

2021

FACULTAD DE POSGRADO

PROPUESTA DEL PROGRAMA DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION PARA EL PROCESO DE GESTION DE TI DE TRANSPORTES SEGUROS S.A.

Trabajo de Titulación presentado en conformidad con los requisitos establecidos para optar por el título de Máster en Gestión del Sistema de Seguridad de la Información.

Profesor guía: Juan Carlos Lopez Molina

Autor: Carlos Guillermo Vargas Álvarez

2021

AGRADECIMIENTOS

Agradezco primero a Dios por la bendición de haberme dado la oportunidad de cursar esta Maestría, agradezco a mis padres por apoyarme siempre e incentivarme en todo momento a ser un mejor profesional, una mejor persona y sobre todo un mejor ser humano.

DEDICATORIA

Este trabajo lo dedico a mis padres, por su esfuerzo diario y su dedicación constante para hacer de mi lo que hoy soy. También lo dedico muy especialmente a mi esposa por estar a mi lado siempre y brindarme su amor, dulzura y paciencia y a mis hijos, por ser el motor que impulsa mi vida día a día.

RESUMEN

Los avances tecnológicos, la transformación digital, los entornos disruptivos y la pandemia por la que la humanidad se encuentra atravesando, han cambiado por completo varios conceptos tradicionales, haciendo que cambiemos nuestra concepción de la seguridad y sobre todo de la seguridad de la información.

Este proyecto consiste en el planteamiento de un Sistema de Gestión de Seguridad de la Información para el proceso de Tecnología en la empresa Transportes Seguros S.A., utilizando como marcos de referencia la ISO 27001, ISO 27002 y NIST.

Se presenta una breve conceptualización de los que es un Sistema de Gestión de Seguridad de la información, así como descripciones breves de la norma ISO 27000 y en detalle ISO 27001 e ISO 27002, y por último una introducción al NIST Cyber Security Framework.

Para conseguir el objetivo buscado, se ha realizado primeramente una evaluación del estado actual de la empresa en el contexto de un SGSI, tomando como base el marco de referencia ISO 27001 e ISO 27002 comparado con el marco de referencia que nos ofrece NIST CSF y realizando una identificación del estado en que se encuentra cada punto o cada control en la organización.

Se identifica los activos críticos de la empresa, de acuerdo con el propio apetito al riesgo definido por la dirección de la organización, para poder priorizar su tratamiento y realizar una evaluación de riesgos, tomando en consideración el marco de referencia Marger IT, orientada a proteger lo que la se ha clasificado como

más importante y que puede causar mayores daños en el caso de ser violadas sus seguridades.

Esta evaluación de riesgos toma en consideración el riesgo inherente, propio del negocio, evalúa los controles existentes, determina el riesgo residual y propone los controles necesarios para mitigar el riesgo residual al momento que las vulnerabilidades existentes sean explotadas.

Finalmente se presenta un Modelo Operacional del SGSI para la implementación de los controles y procedimientos recomendados para garantizar los pilares básicos de la Información y su seguridad, Integridad, Confidencialidad, Disponibilidad y Privacidad.

ABSTRACT

Technological advances, digital transformation, disruptive environments and the pandemic that humanity is going through, have completely changed several traditional concepts, causing us to change our conception of security and especially of information security.

This project consists of the approach to implement an Information Security Management System for the Technology process in the company Transportes Seguros S.A., using ISO 27001, ISO 27002 and NIST as reference frameworks.

A brief conceptualization of what an Information Security Management System is is presented, as well as brief descriptions of the ISO 27000 standard and specifically ISO 27001 and ISO 27002, and finally an introduction to the NIST Cyber Security Framework.

To achieve the objective sought, an evaluation of the current state of the company has been first carried out in the context of an ISMS, based on the ISO 27001 and ISO 27002 reference framework compared to the reference framework offered by NIST CSF and performing an identification of the state of each point or each control in the organization.

The critical assets of the company are identified, according to the risk appetite defined by the organization's management, in order to prioritize their treatment and carry out a risk assessment, taking into consideration the Marger IT framework, aimed at protecting what has been classified as more important and that can cause greater damage in the event of being violated their security.

This risk assessment takes into consideration the inherent risk, typical of the business, assesses the existing controls, determines the residual risk and proposes the necessary controls to mitigate the residual risk when the existing vulnerabilities are exploited.

Finally, an Operational Model of the ISMS is presented for the implementation of the controls and recommended procedures to guarantee the basic pillars of the Information and its security, Integrity, Confidentiality, Availability and Privacy.

INDICE

INDICE DE FIGURAS

1. INTRODUCCIÓN

Transportes Seguros S.A. es una empresa que se encarga del transporte de valores y especies monetarias, como auxiliar del sistema financiero.

Tiene como misión brindar el mejor transporte de valores, operación de cajeros automáticos y administración del efectivo para el sistema financiero.

Su visión es ser la organización líder en el servicio de logística y gestión del efectivo.

La labor de la organización se basa en criterios bien definidos para determinar que el recurso más importante de la organización es el recurso humano, así como que la continuidad del negocio está garantizada por el cumplimiento de leyes y normativas vigentes y teniendo como mandatorio el cumplimiento de los requisitos de seguridad en todas las actividades de la organización.

En la organización el análisis y evaluación de riesgo es una práctica permanente que busca desarrollar una cultura de prevención.

La empresa cuenta actualmente con un Sistema de Gestión Integrado documentado en un Manual, que contiene los procesos a través de los cuales cumple las normativas y políticas en todas sus actividades y los servicios que realiza.

Si bien es cierto que existe un Manual de Gestión Integrado, existen procedimientos que no se encuentran incluidos en el mismo y que han sido incluidos informalmente y su difusión no se ha efectuado de acuerdo con lo establecido en este manual.

El giro propio del negocio de la organización ha obligado a que se efectúen cambios sobre la marcha y al no contar con procedimientos de gestión de cambios, estos han sido efectuados sin el registro y control correspondiente.

La organización cuenta con certificación ISO9001:2015, pero no se ha logrado que sean parte del día a día de la organización y se ha quedado limitado a cumplir para las auditorías respectivas. Esto ha ocasionado que no se tenga un único procedimiento en relación con ciertas actividades que realiza el personal, o que no exista la documentación de un proceso que en la práctica se lleva a cabo en las actividades cotidianas, lo que causa errores y reprocesos e inhabilita la posibilidad de que los controles existentes puedan ser efectivos.

Actualmente la organización no cuenta con un Sistema de Gestión de Seguridad de la información, o con una base inicial en este aspecto, que permita un manejo adecuado de la misma en todas sus formas y que garantice la respectiva Integridad, Confiabilidad, Disponibilidad y Privacidad.

Tomando en cuenta la criticidad de la información que se maneja en la organización, como por ejemplo códigos de apertura de cerraduras digitales, información de rutas y horarios de transporte de efectivo, montos a procesarse, custodiarse y/o transportarse, es imprescindible la implementación de un Sistema de Gestión de Seguridad de la Información, que puede ser parte del Sistema de Gestión Integrado.

El proceso de Gestión de TI, este año ha pasado de ser un proceso de apoyo a ser un proceso estratégico de la organización, debido a que gran parte de la operación está basada en el uso de tecnología y servicios que el proceso entrega, así como la

responsabilidad que recae en el área debido a los privilegios de acceso que tiene la Jefatura, a los sistemas y plataformas que utiliza la organización.

El área de TI, se rige por procedimientos básicos generales que no están en relación a un marco de referencia o estándar propio de TI, de tal forma que los respectivos servicios que esta área entrega a la organización, puedan ser planificados, realizados, verificados y controlados de forma adecuada, esto sumado a la falta del establecimiento de un Gobierno adecuado en el área, hace que se limite la entrega adecuada de la funcionalidad y garantía que debería ofrecer esta área a la organización en general.

Finalmente se debe mencionar que actualmente recae la responsabilidad de administración de todas las plataformas y aplicaciones, como administrador y/o súper usuario, en una sola persona, lo que provoca una alta dependencia funcional, además de generar un riesgo muy alto, tanto para el colaborador, como para la organización.

La solución es la implementación de un Sistema de Gestión de Seguridad de la Información para el proceso de Gestión de TI, que tenga como base, estándares, normas y marcos de referencia reconocidos nacional e internacionalmente, que permitan ejecutar las operaciones diarias de la organización, de acuerdo a procedimientos seguros establecidos, documentados, difundidos, controlados y actualizados que garanticen que la información de la organización cumpla con los siguientes principios, Confidencialidad, Integridad, Disponibilidad y Privacidad.

2. DESARROLLO DEL PROYECTO

2.1 SISTEMA DE GESTIÓN DE SEGURIDA DE LA INFORMACIÓN

Un Sistema de Gestión de Seguridad de la Información es un conjunto de lineamientos, procesos que permiten direccionar el como gestionar los activos de información de una organización con un orden metódico y sistemático, con la finalidad de la consecución de los objetivos de la organización, teniendo como base los riesgos que lo pueden afectar.

2.2 ISO 27000

La norma ISO 27000 nos permite tener una perspectiva general de los Sistemas de Gestión de Seguridad de la información mediante la definición de términos y definiciones utilizados en la familia de normas de seguridad de la información.

2.3 ISO 27001

Es una norma desarrollada por la Organización Internacional de Normalización con el fin de contribuir en la gestión de la Seguridad de la información de las organizaciones.

Su primera versión fue publicada en el año 2005 como una adaptación a la norma británica BS 7799-2. Para el 2013, se tiene la revisión de la norma que introduce un mayor énfasis en la gestión de riesgos y se da un nuevo enfoque a la selección de controles de seguridad. En el 2017 se tiene una nueva revisión de la norma, en la cual se realizan algunas correcciones de términos.

Esta norma aplica a cualquier tipo de empresa, una vez que se haya definido cuan importantes son los activos de información y cuanto es lo que estos aportan en la consecución de sus objetivos.

La norma ISO 27001 es una norma adoptada a nivel mundial para regir la seguridad de la información en las organizaciones.

Figura 1. Adopción de ISO 27001 a nivel mundial

Tomado del sitio (ISO 27001, s.f.)

2.4 ISO 27002

La norma ISO 27002 es una guía con un listado de buenas prácticas en búsqueda de la implantación de controles y medidas de seguridad con base en la experiencia de empresas y organizaciones con reconocimiento mundial.

La norma está compuesta por 14 capítulos subdividido en áreas de seguridad y que lista un total de 114 controles.

2.5 NIST CSF

Es un marco de referencia que busca guiar las actividades de ciberseguridad considerando sus riesgos y su respectiva gestión, pero dejando de lado el uso de estándares rígidos y basándose en varios estándares ya existentes y aceptados como ISO 27001:2013, COBIT 5, entre otros, otorgando una gran simplicidad y flexibilidad.

Proporciona un conjunto de actividades claves para la consecución de resultados específicos de ciberseguridad. Comprende cuatro elementos: funciones, categorías, subcategorías y referencias informativas.

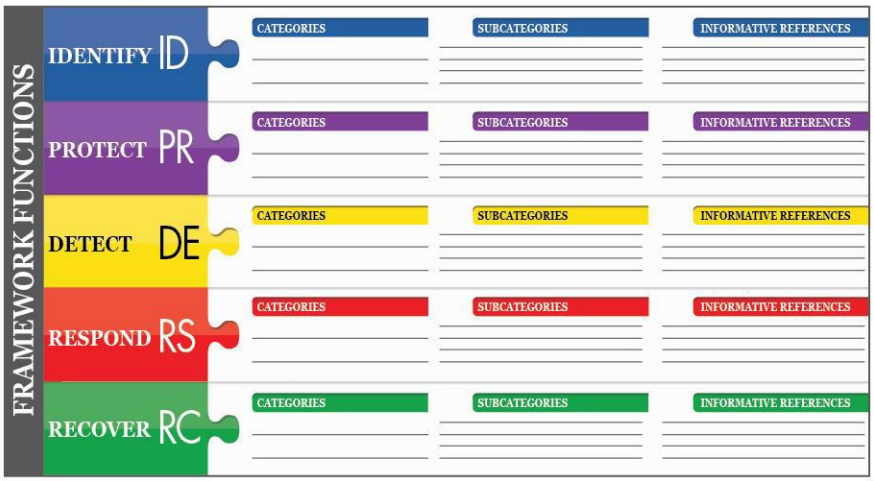

Figura 2. Estructura Framework Core

Tomado del sitio https://doi.org/10.6028/NIST.CSWP.04162018

Las funciones brindan organización para actividades básicas de ciberseguridad y son Identificar, Proteger, Detectar, Responder y Recuperar.

Las Categorías son subdivisiones agrupadas por resultados de ciberseguridad que están vinculados a las necesidades y actividades particulares.

Las Subcategorías, son divisiones aún más pequeñas orientadas a resultados específicos de actividades técnicas o de gestión.

Las Referencias Informativas, son mapeos específicos a otras normas, directrices y prácticas comunes.

2.6 DIAGNÓSTICO

Para obtener un diagnóstico de la situación actual de la empresa Transportes Seguros S.A. en cuanto al Sistema de Gestión de Seguridad de la Información, se tomará como base las Funciones, Categorías y Subcategorías del marco de referencia NIST CSF mapeadas con los puntos y controles de la norma ISO 27001 e ISO 27002, evaluando los procesos de la organización de acuerdo a la siguiente escala de valoración.

ESCALA DE VALORACION		
Etiqueta	**Descripción**	**Valoración**
Inexistente	No se dispone del control o no hay evidencia del mismo.	**0**
Basico	Se evidencia que el control existe pero es básico y no esta documentado.	**1**
Gestionado	Control documentado de forma informal.	**2**
Administrado	Control documentado, aprobado y formalizado.	**3**
Optimizado	Control a más de Administrado, es medido, evaluado y optimizado periódicamente	**4**

Figura 3. Escala de Valoración

Mediante la cual se evaluará la madurez de los procesos existentes, o no, en la organización en comparación con los sugeridos por NIST CSF, ISO 27001 e ISO 27002.

Esto nos permitirá obtener ciertas oportunidades de mejora y tener una ponderación por subcategoría, mediante la cual podemos observar cuales son los puntos más bajos en relación de la madurez de los diferentes procesos, esto para cada categoría y a su vez visualizar la evaluación por las diferentes Funciones de NIST CSF.

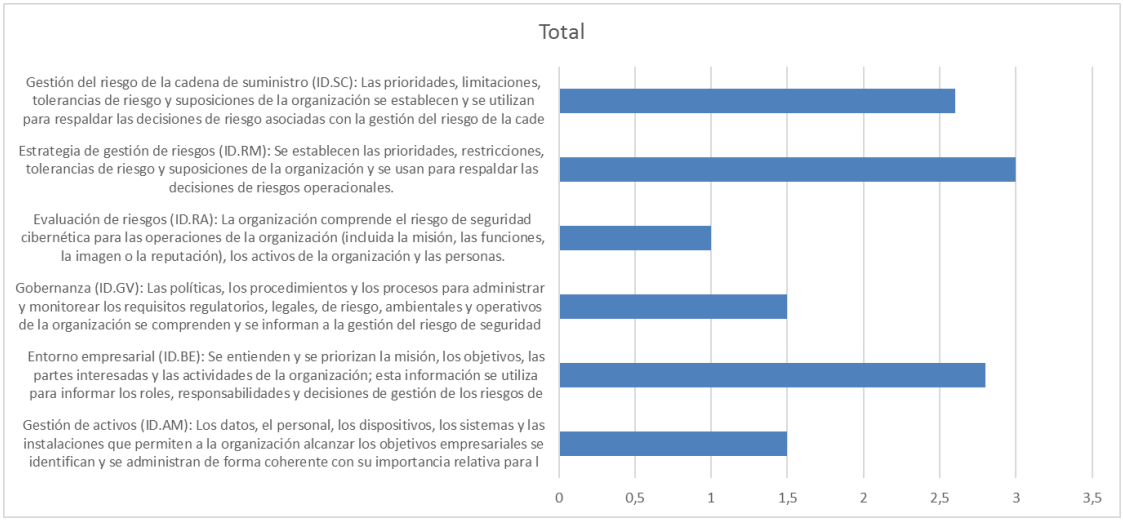

Figura 4. Valoración Función Identificar

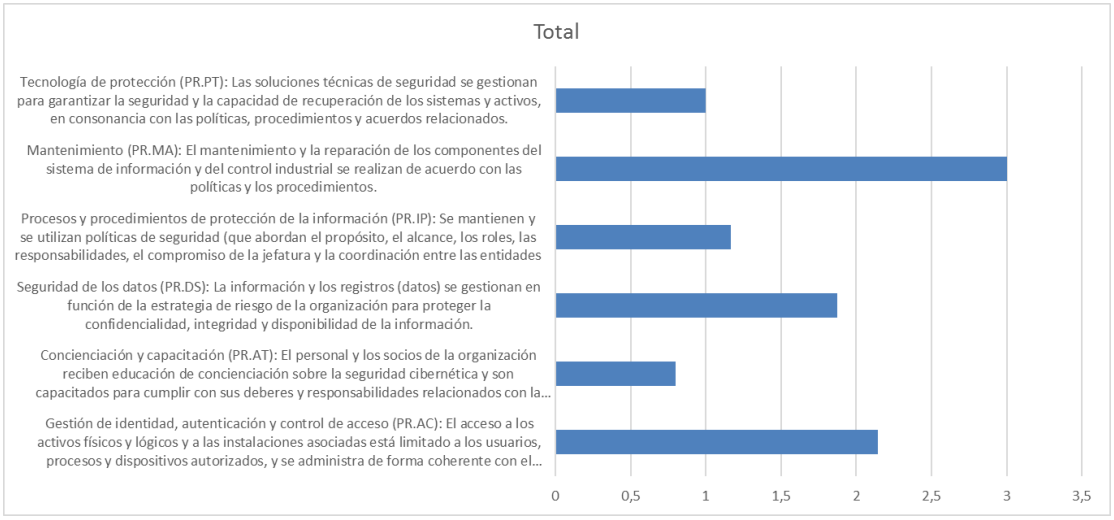

Figura 5. Valoración Función Proteger

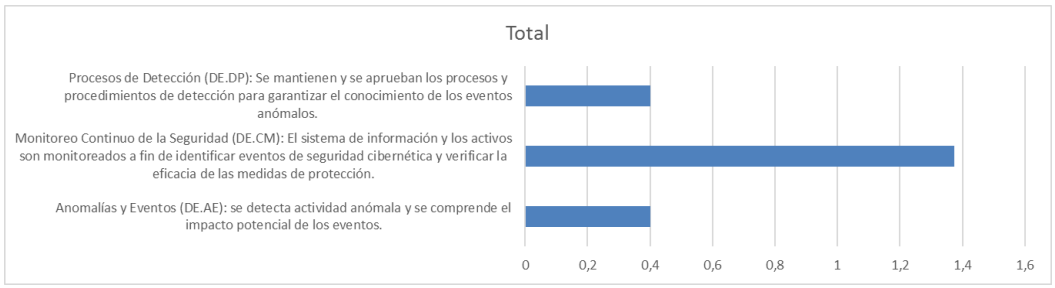

Figura 6. Valoración Función Detectar

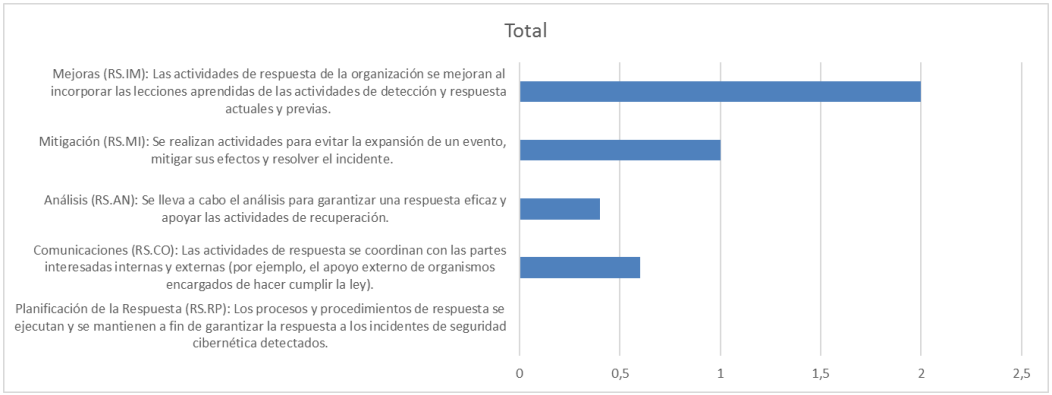

Figura 7. Valoración Función Responder

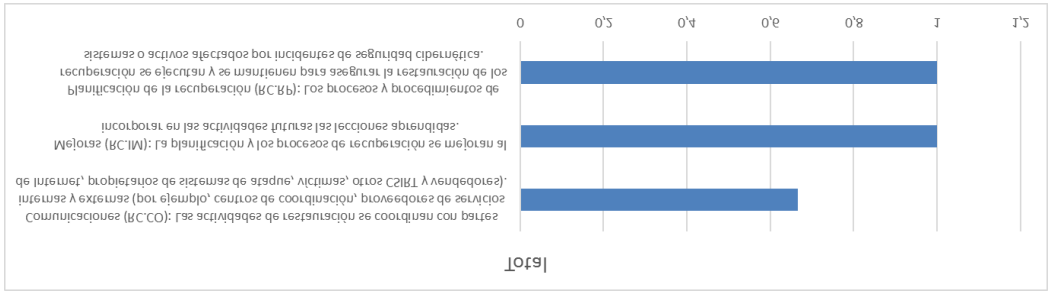

Figura 8. Valoración Función Recuperar

Y finalmente tener una valoración consolidada en relación a todas las funciones del marco de referencia NIST CSF, con las respectivas conclusiones.

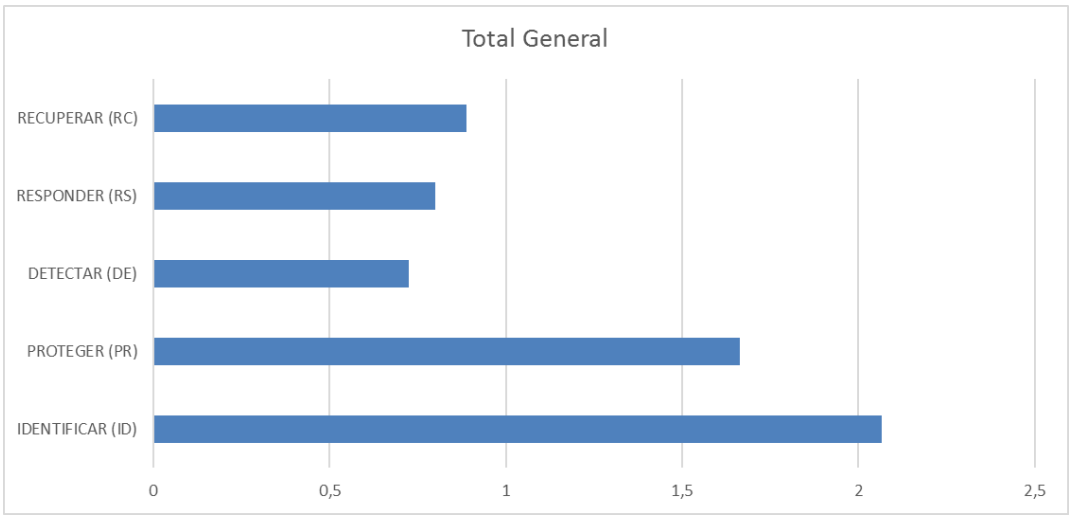

Figura 9. Valoración General por Funciones de NIST CSF

CONCLUSIÓN
Es imprescindible implementar un Sistema de Gestión de Seguridad de la Información por el tipo de información procesada, actualmente la organización cuenta con procedimientos y controles generales, pero que deben ser analizados, actualizados y orientados hacia el SGSI, adicional al desarrollo e implementación de políticas y procedimientos inexistentes.
Se debe dar prioridad a establecer las políticas y procedimientos necesarios para la detección de eventos de seguridad de la información, así como a las políticas y procedimientos de respuesta y recuperación ante la materialización de los mismos, buscando la mejora conínua para garantizar la cotinuidad de la organización y sus sistemas y activos.

Figura 10. Conclusiones de la fase de Diagnóstico

2.7 CLASIFICACION DE INFORMACIÓN

Se procede a realizar una clasificación de la información tomando en cuenta las entidades que en la organización se han visualizado de acuerdo a un modulador de

riesgo proporcionado por la dirección y teniendo en cuenta los principios de Confidencialidad, Integridad, Disponibilidad y Privacidad de la Información.

Escala de Impacto		
Denominación	Valor	Descripción
Catastrofico	9 a 10	Impacto catastrófico
Mayor	7 a 8	Impacto muy grave
Moderado	5 a 6	Impacto de importancia
Menor	3 a 4	Impacto menor
Insignificante	1 a 2	Impacto nulo

Probabilidad de Ocurrencia	
Certeza	100%
Probable	80%
Posible	60%
Poco probable	40%
Raro	20%

Impacto	Catastrófico	Mayor	Moderado	Menor	Insignificante
Tipología del impacto					
Pérdidas Financieras	> a 500.000	500.000 a 100.000	100.000 a 50.000	50.000 a 10.000	< a 10.000
Interrupción de operaciones total y/o parcial	> a 1 semana	1 semana a 2 dias	2 dias a 8 horas	8 horas a 2 horas	< a 2 horas
Pérdida Reputacional	Conocimiento internacional	Conocimiento nacional	Conocimiento local	Conocimiento interno	Conocimiento de directivos
Gestión Humana	Pérdida de vidas humanas / incapacidad 6 meses	Incapacidad de 6 meses a 3 meses	Incapacidad de 3 meses a 1 mes	Incapacidad de 1 mes a 3 dias	Sin lesiones / incapacidad hasta 3 días

Figura 11. Modulador del Riesgo

Al determinar los activos de información de la organización y clasificarlos, podemos obtener un panorama claro de los actores de los diferentes procesos que se ejecutan dentro y fuera, así como la información que producen y/o procesan y su importancia ante consecución de los objetivos estratégicos.

ENTIDAD	NOMBRE DEL TIPO DE INFORMACION	DEFINICIÓN DEL TIPO DE INFORMACIÓN	ACTIVO DE INFORMACIÓN	FORMATO	PROCESOS QUE UTILIZAN EL ACTIVO	PROPIETARIO DEL ACTIVO	PÉRDIDAS FINANCIERA				INTERRUPCIÓN OPERACIONE				PÉRDIDA REPUTACION				GESTIÓN HUMANA				TOTAL
							CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	PRIVACIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	PRIVACIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	PRIVACIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	PRIVACIDAD	
Organización	Catálogo de productos & servicios	Información de los productos y servicios que ofrece la organización	Manual Integrado	Digital	Todos	Dirección																	
	Información de ubicabilidad	Información que identifica geográficamente a la organización, como oficina principal, sucursal y ubicaciones satélites	Carpeta compartida Dpto Legal	Digital	Todos	Legal																	
			Archivo Físco Dpto Legal	Físico	Todos	Legal																	
			Base de datos CarsyncFleet	Digital	Operaciones, Canales, TI	TI																	
	Información tributaria	Información de identificación ante entidades regulatorias	Carpeta compartida Dpto Legal	Digital	Logísitica, Contabilidad	Legal																	
			Archivo Físco Dpto Legal	Físico	Todos	Legal																	
	Información legal	Información que contiene permisos de funcionamiento ante entes regulatorios y estatutarios	Carpeta compartida Dpto Legal	Digital	Legal	Legal																	
			Archivo Físco Dpto Legal	Físico	Todos	Legal																	
	Información bancaria	Información que contiene datos de cuentas bancarias de la organización	Base de datos de contabilidad	Digital	Contabilidad	Legal																	

Figura 12. Clasificación de Activos

Proveedores	Catálogo de productos & servicios	Información de los productos y servicios que ofrece el proveedor	Base de datos de proveedores	Digital	Logística, Contabilidad, Inventarios	Contabilidad	
	Información de ubicabilidad	Información que identifica geográficamente al proveedor	Base de datos de proveedores	Digital	logística, Contabilidad	Contabilidad	
	Información tributaria	Información de identificación del proveedor ante entidades regulatorias	Base de datos de contabilidad	Digital	Contabilidad	Contabilidad	
	Información legal	Contrato de prestación de servicios y SLAS del proveedor	Carpeta compartida Dpto Legal	Digital	Contabilidad, Legal, TI	Legal	
	Información bancaria	información de cuentas bancarias del proveedor	Base de datos de contabilidad	Digital	Contabilidad	Contabilidad	
Clientes	Información de ubicabilidad General	Información que identifica geográficamente al cliente	Base de datos de clientes	Digital	Contabilidad, Operaciones, Canales	Contabilidad	
	Información de ubicabilidad específica	Información que identifica geográficamente las ubicaciones del cliente que son atendidas por la organización	Base de datos CarsyncFleet	Digital	Operaciones, Canales	Operaciones	
			Archivo de excel de Canales	Digital	Operaciones, Canales	Canales	
	Información tributaria	Información de identificación del proveedor ante entidades regulatorias	Base de datos de contabilidad	Digital	Contabilidad	Contabilidad	
	Información legal	Contrato de prestación de servicios y SLAS de la organización frente al cliente	Carpeta compartida Dpto Legal	Digital	Operaciones, Canales, Legal	Legal	
	Información bancaria	Información con datos de cuentas bancarias de los clientes	Base de datos de contabilidad	Digital	Contabilidad	Contabilidad	
	Requerimientos de transporte de valores	Información con los requerimientos de cantidades y sitios a los que se debe tranasportar valores de los clientes por parte de la organización	Correo Electrónico	Digital	Canales, Operaciones	Canales	
			Archivo de excel de planificación de operación	Digital	Operaciones	Operaciones	
			Archivo de excel de ejecutado de la operación	Digital	Operaciones	Operaciones	
			Hoja de control de ejecutado de la operación	Físico	Operaciones	Operaciones	
			Guias de transporte de valores	Físico	Operaciones, Canales, Procesamiento del Efectivo, Contabilidad	Operaciones	
	Requerimientos de procesamiento de efectivo	Información de catidades de dinero de los clientes que se debe procesar	Correo Electrónico	Digital	Canales, Operaciones	Canales	
			Archivos de excel de procesamiento de efectivo	Digital	Procesamiento del Efectivo, Canales, Financiero	Procesamiento del Efectivo	
			Guias de transporte de valores	Físico	Operaciones, Canales, Procesamiento del Efectivo, Contabilidad	Operaciones	
Empleados	Información de ubicabilidad	Información con datos para ubicabilidad de los empleados	Carpeta compartida RRHH	Digital	RRHH, Operaciones, Legal	RRHH	
	Información personal	Información que contiene datos personales de los empleados	Carpeta compartida RRHH	Digital	RRHH, Legal	RRHH	
			Base de datos RRHH	Digital	RRHH, Legal	RRHH	
			Archivo Físico RRHH	Físico	RRHH, Legal, Dpto. Médico		
	Información tributaria	Información de identificación de los empleados ante entes regulatorios	Carpeta compartida RRHH	Digital	Contabilidad, RRHH, Legal	RRHH	
			Archivo Físico RRHH	Físico	Contabilidad, RRHH, Legal	RRHH	
	Información legal	Información de carácter legal de los empleados, como contratos, juicios, convenios de confidencialidad	Carpeta compartida RRHH	Digital	RRHH, Legal	Legal	
			Archivo Físico RRHH	Físico	RRHH, Legal	Legal	
	Información bancaria	Información de cuentas bancarias y financiera de los empleados	Carpeta compartida RRHH	Digital	Contabilidad, RRHH, Legal	RRHH	
			Base de datos RRHH	Digital	Contabilidad, RRHH, Legal	RRHH	
	Ficha médica	información con datos médicos, historial de enfermedades y seguimiento y control de las mismas	Registro médico	Digital	Dpto. Médico	Dpto. Médico	
			Archivo Físico Dpto. Médico	Físico	Dpto. Médico	Dpto. Médico	
	Historial Laboral	Información con record laboral del empleado	Carpeta compartida RRHH	Digital	RRHH, Legal	RRHH	
			Archivo Físico RRHH	Físico	RRHH, Legal	RRHH	
Cerraduras	Información de ubicabilidad	Información con datos para ubicación geográfica de cerraduras instaladas en clientes por parte de la organización	Base de datos SGSSqlServer	Digital	Operaciones	TI	
			Base de datos Pambox3SQL	Digital	Operaciones	TI	
	Información de identificación	Información con datos para identificación de cerraduras instaladas en clientes por parte de la organización	Base de datos SGSSqlServer	Digital	Operaciones	TI	
			Base de datos Pambox3SQL	Digital	Operaciones	TI	
	Información de transaccionalidad	Información con registro de eventos de operación de cerraduras	Base de datos SGSSqlServer	Digital	Operaciones, TI	TI	
	Información especializada	Información referente a claves estáticas para apertura de cerraduras	Base de datos Pambox3SQL	Digital	Operaciones, TI	TI	
Blindados	Información de ubicabilidad	Información con datos para ubicación geográfica de vehículos blindados de la organización	Base de datos IMWARE	Digital	Operaciones	TI	
			Base de datos CMSV6	Digital	Operaciones	TI	
			Base de datos CarsyncFleet	Digital	Operaciones, TI	TI	
	Información de identificación	Información con datos para identificación de vehículos blindados de la organización	Base de datos IMWARE	Digital	Operaciones	TI	
			Base de datos CMSV6	Digital	Operaciones, TI	TI	
			Base de datos CarsyncFleet	Digital	Operaciones, TI	TI	
			Archivo Excel de Inventario de Dispositivos de Blindados	Digital	Operaciones, TI, Legal	TI	
	Información especializada	Información en tiempo real de ubicación y estado de vehículos blindados de la organización	Base de datos IMWARE	Digital	Operaciones, TI	TI	
			Base de datos CMSV6	Digital	Operaciones, TI	TI	
Sectores / Rutas	Información de ubicabilidad	Información con datos geográficos de rutas y sectores por donde circulan los vehículos blindados de la organización	Base de datos CarsyncFleet	Digital	Operaciones	TI	
			Archivo de excel de planificación de operación	Digital	Operaciones	Operaciones	
			Archivo de excel de ejecutado de la operación	Digital	Operaciones	Operaciones	
	Información de identificación	Información con datos para identificación de sectores y rutas por donde circulan vehículos blindados de la organización	Base de datos CarsyncFleet	Digital	Operaciones	TI	
			Archivo de excel de planificación de operación	Digital	Operaciones	Operaciones	
			Archivo de excel de ejecutado de la operación	Digital	Operaciones	Operaciones	
	Información específica	Información relacionada con requerimientos a ser atendidos en las rutas y sectores que atiende la organización	Archivo de excel de planificación de operación	Digital	Operaciones	Operaciones	
			Archivo de excel de ejecutado de la operación	Digital	Operaciones	Operaciones	

Figura 13. Clasificación de Activos

2.8 INVENTARIO DE ACTIVOS DE INFORMACIÓN

Una vez que se tiene a todos los activos de información de la organización identificados, clasificados y evaluados, se procede a determinar aquellos activos que sean de mayor importancia para la organización, y que pueden ocasionar, en el caso de que alguna vulnerabilidad sea explotada mayor riesgo a la continuidad del negocio. De esta manera se obtiene los activos calificados como críticos para que sean tratados con la prioridad que ameritan.

ACTIVO DE INFORMACIÓN	NOMBRE DEL TIPO DE INFORMACION	DEFINICIÓN DEL TIPO DE INFORMACIÓN	FORMATO	PROPIETARIO DEL ACTIVO	CRITICIDAD
Carpeta compartida Dpto Legal	Información legal	Información que contiene permisos de funcionamiento ante entes regulatorios y estatutarios	Digital	Legal	
Archivo Físco Dpto Legal			Físico	Legal	
Carpeta compartida Dpto Legal	Información legal	Contrato de prestación de servicios y SLAS de la organización frente al cliente	Digital	Legal	
Correo Electrónico	Requerimientos de transporte de valores	Información con los requerimientos de cantidades y sitios a los que se debe tranasportar valores de los clientes por parte de la organización	Digital	Canales	
Archivo de excel de planificación de operación			Digital	Operaciones	
Archivo de excel de ejecutado de la operación			Digital	Operaciones	
Hoja de control de ejecutado de la operación			Físico	Operaciones	
Correo Electrónico	Requerimientos de procesamiento de efectivo	Información de catidades de dinero de los clientes que se debe procesar	Digital	Canales	
Archivos de excel de procesamiento de efectivo			Digital	Procesamiento del Efectivo	
Base de datos SGSSqlServer	Información de ubicabilidad	Información con datos para ubicación geográfica de cerraduras instaladas en clientes por parte de la organización	Digital	TI	
Base de datos Pambox3SQL			Digital	TI	
Base de datos SGSSqlServer	Información de identificación	Información con datos para identificación de cerraduras instaladas en clientes por parte de la organización	Digital	TI	
Base de datos Pambox3SQL			Digital	TI	
Base de datos SGSSqlServer	Información de transaccionalidad	Información con registro de eventos de operación de cerraduras	Digital	TI	
Base de datos Pambox3SQL	Información especializada	Información referente a claves estáticas para apertura de cerraduras	Digital	TI	

Figura 14. Clasificación de Activos Críticos

Base de datos IMWARE	Información de ubicabilidad	Información con datos para ubicación geográfica de vehículos blindados de	Digital	TI	
Base de datos CarsyncFleet			Digital	TI	
Archivo de excel de planificación de operación			Digital	Operaciones	
Base de datos CarsyncFleet	Información de identificación	Información con datos para identificación de sectores y rutas por donde circulan vehículos blindados	Digital	TI	
Archivo de excel de planificación de operación			Digital	Operaciones	
Archivo de excel de planificación de operación	Información específica	Información relacionada con requerimientos a ser atendidos en las rutas y sectores que atiende la organización	Digital	Operaciones	

Figura 15. Clasificación de Activos Críticos

2.9 EVALUACIÓN DE RIESGOS – ANÁLISIS DE VULNERABILIDADES

Teniendo ya identificados los activos críticos, se procede a realizar una Evaluación de Riesgos de estos activos. En este caso se ha tomado como referencia para la evaluación a Marger IT y se evaluará el riesgo inherente, de acuerdo con la probabilidad e impacto.

Identificación posibles vulnerabilidades	Riesgo Inherente	Controles Existentes	Tipo de	Riesg	Plan de Acción
Falta de controles en BDD		Procedimiento de revisión de BDD y Servidores	Manual		Implementar procedimiento para el control de BDD y formalizar los controles actuales
Asignación de privilegios erronea		Procedimiento para cuentas de usuario	Manual		Implementación de procedimiento de asignación de roles y responsabilidades, Implementación de Directorio Activo
Inadecuados procedimientos de control de acceso		Procedimiento para seguridad tecnológica, procedimiento para cuentas de usuario	Manual		Implementación de procedimiento específico y completo para el control de accesos
Inexistencia de procedimientos de recuperación		Política de continuidad del negocio	Manual		Actualización de política de continuidad del negocio y gestión de riesgos
Control inadecuado del acceso físico		Procedimientos de control de ingreso físico	Automático		Actualizar procedimientos de control de ingreso físico orienándolos hacia la seguridad de lainformación
Inadecuados procedimientos de control de acceso		Procedimiento para seguridad tecnológica, procedimiento para cuentas de usuario	Manual		Implementación de procedimiento específico y completo para el control de accesos
Metodos de autenticación débiles		Procedimiento para cuentas de usuario	Manual		Actualización de procedimiento para cuentas de usuario, incluyendo nuevos métodos de autenticación con múltiple

Figura 16. Evaluación de Riesgos

Una vez obtenida la valoración para el riesgo inherente, se revisa los controles que se tienen actualmente para la respectiva mitigación del riesgo y se obtiene una valoración del riesgo residual, ante el cual se proponen los controles que busquen mitigar este riesgo.

N	ID-PA	Plan de Acción	Prioridad	Tipo de Control	2021		2022									
					NOV	DIC	ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT
3	PA-003	Implementación de procedimiento de monitoreo permanente de BDD		Automático												
4	PA-004	Implementación de procedimiento de asignación de roles y responsabilidades, Implementación de Directorio Activo		Automático												
10	PA-010	Implementar procedimiento para el control de BDD y formalizar los controles actuales		Automático												
5	PA-005	Implementar procedimiento para el monitoreo de usuarios y formalizar los controles actuales		Automático												
7	PA-007	Implementación de procedimiento para control de logs de BDD		Automático												
9	PA-009	Implementación de procedimiento específico y completo para el control de accesos		Automático												
17	PA-017	Actualizar y mejorar el procedimiento para cuentas de usuario orientándolo hacia la seguridad de la información		Manual												
6	PA-006	Implementar plan de campañas para concientizar a los usuarios sobre seguridad		Manual												
11	PA-011	Actualización de política de continuidad del negocio y gestión de riesgos		Manual												
12	PA-012	Actualizar procedimientos de control de ingreso físico orienándolos hacia la seguridad de lainformación		Automático												
13	PA-013	Implementar procedimiento para revisión de configuraciones y simulacros de funcionamiento de BDD		Automático												
15	PA-015	Actualización de procedimiento para cuentas de usuario, incluyendo nuevos métodos de autenticación con múltiple factor de autenticación		Automático												
16	PA-016	Implementar política para regular y controlar la gestion del servicio de red por parte del proveedor		Automático												
18	PA-018	Actualizar procedimiento para seguridad tecnológica, orientándolo a seguridad de la información, utilizar criterio del menor privilegio		Automático												
19	PA-019	Implementación de procedimiento y controles de revisión continua de privilegios de usuarios		Automático												
20	PA-020	Actualizar procedimientos e incluir política sobre uso de contraseñas predeterminadas		Manual												
1	PA-001	Implementación de un procedimiento de de capacitación permanente		Manual												
2	PA-002	Mejora de procedimiento de contratación, Implementación de procedimiento de Evaluación de desempeño		Manual												
8	PA-008	Revisar y actualizar procedimientos de auditoría interna y orientarlos hacia seguridad de la información		Manual												
14	PA-014	Implementación de DLP y procedimiento para el monitoreo del DLP		Automático												
21	PA-021	Implementar procedimiento específico para el control sobre los datos de entrada y salida		Automático												
22	PA-022	Implementar campañas de motivación e integración del personal regulares		Manual												
23	PA-024	Actualizar sanciones de reglamento interno orientadas a eventos de seguridad de la información		Manual												
24	PA-023	Actualizar convenios de confidencialidad con criterios de seguridad de la infromación		Manual												

Figura 17. Planes de Acción

2.10 DOCUMENTOS CLAVE DEL SGSI

Es muy importante para el Sistema de Gestión de Seguridad de la Información la definición de políticas de alto nivel, que cuente con un lineamiento de responsables de ejecución, así como la priorización de dichas políticas, para que se pueda construir el sistema de acuerdo con las necesidades más prioritarias de la organización.

POLITICAS DE SEGURIDAD DE LA INFORMACION				
ID-ISO	**POLÍTICA**	**DESCRIPCIÓN**	**RESPONSABLE**	**PRIORIDAD**
A6.2.1	Política de dispositivos móviles	Difinición de lineamientos en el uso de dispositivos móviles de la organización para asegurar la información que contienen	Riesgos / Jefe de TI	
A6.2.2	Teletrabajo	Definición de lineamientos en el teletrabajo para garantizar el aseguramiento de la infromación proccesada	Riesgos / Jefe de TI	
A8.2.1	Clasificación de la información	Definición de procedimientos que guían la forma de realizar la clasificación de la información de la organización, su control y actualización	Riesgos	
A9.1.1	Política de control de acceso	Definición de medidas técnicas y organizativas relacionadas con los permisos de acceso a sistemas que albergan la información de la organización, así como el acceso a la propia información	Riesgos	
A9.1.2	Acceso a las redes y a los servicios de red	Definición de medidas técnicas relacionadas con los permisos de acceso a las redes y a los servicios de red	Riesgos / Jefe de TI	
A9.2.2	Provisión de acceso de usuario	Definición de los lineamientos para el otorgamiento de acceso de usuario a los diferentes activos que procesan información de la orgnización	Riesgos / Jefe de TI	
A9.2.3	Gestión de privilegios de acceso	Definición de procedimientos para la gestión de los privilegios de acceso	Riesgos / Jefe de TI	
A9.2.4	Gestión de la información secreta de autenticación de los usuarios	Definición de procedimientos para la gestión de la información secreta de autenticación de los usuarios	Riesgos / Jefe de TI	
A9.2.5	Revisión de los derechos de acceso de usuario	Definición de procedimientos para la revisión y control de los de rechos de acceso de los usuarios	Jefe de TI	
A9.2.6	Retirada o reasignación de los derechos de acceso	Definición de procedimientos para retirar o reasignar los derechos de acceso de los usuarios	Jefe de TI	
A9.3.1	Uso de la información secreta de autenticación	Definición de procedimientos para el control del uso de la información secreta de autenticación	Riesgos / Jefe de TI	
A12.3.1	Copias de seguridad de la información	Definición de procedimientos para controlar y asegurar las copias de seguridad de la información de la organización	Jefe de TI	
A6.1.1	Roles y responsabilidades en seguridad de la información	Definición de roles y responsabilidades de todos los involucrados en el SGSI	Riesgos	
A7.2.1	Responsabilidades de gestión	Definición de las responsabilidades de los involucrados en la gestión del SGSI	Riesgos	
A8.1.1	Inventario de activos	Definición de procedimientos para la realización, actualización, control y monitoreo del inventario de activos	Riesgos / Jefe de TI	
A8.1.2	Propiedad de los activos	Definición de los propietarios de los diferentes activos de la organización	Riesgos	
A9.2.1	Registro y baja de usuario	Definción de proccedimientos a realizarse para el registro y dada de baja de los usuarios	Jefe de TI	
A10.1.2	Gestión de claves	Definición de procedimientos para la gestión de claves de los sistemas de uso de la organización	Jefe de TI	
A13.2.3	Mensajería electrónica	Definición de procedimientos para el control del uso correcto de la mensajería electrónica	Riesgos / Jefe de TI	
A16.1.3	Notificación de puntos débiles de la seguridad	Definición de procedimientos para establecer la forma, medios y canales de notificación de los puntos débiles de la seguridad	Jefe de TI	
A5.1.1	Políticas para la seguridad de la información	Descripción de alcance de la política de seguridad de la información, sus objetivos, responsables y su cumplimiento	Riesgos	

A6.1.2	Segregación de tareas	Política que describe las tareas que cada uno de los involucrados en el SGSI deberán ejecutar	Riesgos	
A8.1.3	Uso aceptable de los activos	Definición de lineamientos que regulan el uso aceptable de los activos de la organización	Riesgos	
A8.1.4	Devolución de activos	Definición de procedimientos que orientan el accionar de la organización ante una devolución de activos	Jefe de TI	
A8.2.2	Etiquetado de la información	Definición de procedimientos para la ejecución, control y monitoreo del etiquetado de información	Riesgos	
A8.2.3	Manipulado de la información	Definición de procedimientos que regulan y controlan la manipulación de la información de la organización	Riesgos	
A8.3.1	Gestión de soportes extraíbles	Definición de procedimientos que regulan, controlan y monitorean la gestión de soportes extraibles para asegurar la información que contienen	Jefe de TI	
A8.3.2	Eliminación de soportes	Definición de procedimientos para la eliminación de soportes	Riesgos / Jefe de TI	
A8.3.3	Soportes físicos en tránsito	Definición de procedimientos que regulan, controlan y moitorean los soportes físicos en tránsito	Riesgos / Jefe de TI	
A9.4.1	Restricción del acceso a la información	Definición de lineamientos para el control y restricción del acceso a la infromación	Riesgos / Jefe de TI	
A9.4.2	Procedimientos seguros de inicio de sesión	Definición de procedimientos seguros de inicio de sesión	Jefe de TI	
A11.1.1	Perímetro de seguridad física	Definición de procedimientos para el control de la seguridad física del perímetro de la organización	Riesgos / Seguridad Física	
A11.1.2	Controles físicos de entrada	Definición de procedimientos que controlan el acceso físico a las instalaciones de la organización	Riesgos / Seguridad Física	
A11.2.1	Emplazamiento y protección de equipos	Definición de lineamientos para la protección de los equipos de la organización	Jefe de TI	
A11.2.3	Seguridad del cableado	Definición de procedimientos para controlar y asegurar el cableado, instalación, mantenimiento y uso	Jefe de TI	
A11.2.4	Mantenimiento de los equipos	Definición de procedimientos para el correcto mantenimiento de los equipos de la organización	Jefe de TI	
A11.2.6	Seguridad de los equipos fuera de las instalaciones	Definición de procedimientos para garantizar la seguridad de los equipos fuera de las instalaciones de la organización	Riesgos / Jefe de TI	
A11.2.7	Reutilización o eliminación segura de equipos	Definición de procedimientos para asegurar la reutilización o eliminación de equipos de la organización	Jefe de TI	
A11.2.8	Equipo de usuario desatendido	Definición de procedimientos para evitar la fuga de información o el mal uso de un equipo desantendido	Riesgos / Jefe de TI	
A11.2.9	Política de puesto de trabajo despejado y pantalla limpia	Definición de lineamientos para garantizar que los puestos de trabajo estén despejados, ordenados y se mantengan las pantallas con lo estrictamente necesario	Riesgos / Jefe de TI	
A12.1.2	Gestión de cambios	Definición de procedimientos para determinar una correcta gestión de cambios, garantizando la trazabilidad	Riesgos / Jefe de TI	
A12.4.1	Registro de eventos	Definición de procedimientos para registrar los detalles de eventos materializados	Riesgos / Jefe de TI	
A12.6.1	Gestión de las vulnerabilidades técnicas	Definición de procedimientos para el análisis, control y gestión de las vulnerabilidades técnicas	Jefe de TI	
A12.6.2	Restricción en la instalación de software	Definición de procedimientos y controles para la restricción de instalación de software	Jefe de TI	

A12.7.1	Controles de auditoría de sistemas de información	Definición de procedimientos para el establecimiento de controles de audtoría de sistemas de infromación	Riesgos / Jefe de TI	
A13.1.1	Controles de red	Definición de procedimientos para el establecimiento de controles para el aseguramiento de la red	Jefe de TI	
A13.1.2	Seguridad de los servicios de red	Definición de procedimientos para el establecimiento de la seguridad de los servicio de red	Jefe de TI	
A13.1.3	Segregación en redes	Establecimiento de lineamientos y ejecución de segración de las redes de datos de la organización	Jefe de TI	
A14.1.3	Protección de las transacciones de servicios de aplicaciones	Definición de procedimientos para proteger las transacciones de servicio de aplicaciones	Jefe de TI	
A14.2.8	Pruebas funcionales de seguridad de sistemas	Defínción de planes de pruebas funcionales para garantizar la segurida de los sistemas	Jefe de TI	
A16.1.2	Notificación de los eventos de seguridad de la información	Definición de procedimientos para establecer la forma, medios y canales de notificación de los eventos de seguridad de la información	Jefe de TI	
A16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	Definición de procedimientos para evaluar y tomar decisiones frente a eventos de seguridad de la información que han sido materializados	Riesgos / Jefe de TI	
A16.1.5	Respuesta a incidentes de seguridad de la información	Definición de procedimientos para la respuesta efectiva ante incidentes de seguridad de la infromación que se han materializado	Riesgos / Jefe de TI	
A16.1.7	Recopilación de evidencias	Definición de procedimientos para establecer parámetros adecuados para el recopilación de las evidencias	Riesgos / Jefe de TI	
A17.1.2	Implementar la continuidad de la seguridad de la información	Definición de procedimientos en búsqueda de mantener la continuidad de la seguridad de la información	Riesgos / Jefe de TI	
A18.2.2	Cumplimiento de las políticas y normas de seguridad	Definición de procedimientos para el control y evaluación del cumplimiento de las políticas y normas de seguridad	Riesgos	
A18.2.3	Comprobación del cumplimiento técnico	Definición de procedimientos para el control del cumplimiento de aspectos técnicos	Riesgos / Jefe de TI	
A6.1.3	Contacto con las autoridades	Definir los canales de comunicación y la forma para informar a las autoridades de todo lo referente al SGSI	Riesgos	
A7.2.2	Concienciación, educación y capacitación en seguridad de la información	Definición de procedimientos orientados a conseguir que todos los involucrados en el SGSI tengan conciencia y estén bien capacitados sobre seguridad de la información	Riesgos	
A7.2.3	Proceso disciplinario	Definición de lineamientos en cuanto al reglamento interno, con acciones y sanciones definidas	RRHH	
A11.2.2	Instalaciones de suministro	Definición de procedimientos para garantizar las instalaciones de suministro de la organización	Jefe de TI	
A12.2.1	Controles contra el código malicioso	Definición de procedimientos para controlar y evitar la existencia de código malicioso	Jefe de TI	
A14.2.2	Procedimiento de control de cambios en sistemas	Definición de procedimientos para el establecimiento de controles para los cambios de sistemas	Jefe de TI	
A14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	Definición de procedimientos para realizar las revisiones ténicas de las plaicaiones cuando se han realizado cambios en el sistema operativo de los equipos de la organización	Jefe de TI	
A14.2.7	Externalización del desarrollo de software	Definición de procedimientos para el control y aseguramiento del desarrollo de software realizado externamente	Riesgos / Jefe de TI	
A14.2.9	Pruebas de aceptación de sistemas	Definición de planes de pruebas previas a la aceptación e implementación de cualquier sistema	Riesgos / Jefe de TI	
A14.3.1	Protección de los datos de prueba	Definición de lineamientos para garantizar la protección de los datos de prueba en el desarrollo de aplicaciones	Riesgos / Jefe de TI	

A15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	Definición de procedimientos para el control y monitoreo de la cadena de suministro de tecnología de la información y de las comunicaciones	Riesgos / Jefe de TI	
A16.1.6	Aprendizaje de los incidentes de seguridad de la información	Definición de procedimientos para explotar las lecciones que nos dejan los incidentes de seguridad de la información en búsqueda de la mejora contínua	Jefe de TI	
A17.1.1	Planificación de la continuidad de la seguridad de la información	Definición de procedimientos para el análisis y planificación de la continnuidad de la seguridad de la información	Riesgos / Jefe de TI	
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Definición de procedimientos que permiten la verificación, revisión y evaluación permanente de la continuidad de la seguridad de la información	Riesgos / Jefe de TI	
A18.2.1	Revisión independiente de la seguridad de la información	Definición de lineamientos para la ejecución de revisiones independientes al sistema de gestión de seguridad de la información	Riesgos	

Figura 18. Políticas de Alto Nivel

Por otro lado es necesario establecer el Modelo operacional del SGSI, para poder contar con el detalle de los procedimientos que se deben implementar, sus métricas con las cuales se debe evaluar su cumplimiento, los responsables de la implementación de estos procedimientos, así como las fechas en las cuales está planificado llevar a cabo las acciones, el presupuesto que será necesario para la implementación y el estado de la actividad.

Categoría	Codigo	Fuente	Nombre	Descripción
Técnico	PA-003	Evaluación de Riesgos	Monitoreo de BDD	Implementación de procedimiento de monitoreo permanente de BDD
Gestión	PA-004-a	Evaluación de Riesgos	Asignación de Roles y Responsabilidades	Implementación de procedimiento de asignación de roles y responsabilidades,
Técnico	PA-004-b	Evaluación de Riesgos	Directorio Activo	Implementación de Directorio Activo
Técnico	PA-010	Evaluación de Riesgos	Control de BDD	Implementar procedimiento para el control de BDD y formalizar los controles actuales
Técnico	PA-005	Evaluación de Riesgos	Monitoreo de Usuarios	Implementar procedimiento para el monitoreo de usuarios y formalizar los controles actuales
Técnico	PA-007	Evaluación de Riesgos	Monitore de logs de BDD	Implementación de procedimiento para control de logs de BDD
Gestión	PA-009	Evaluación de Riesgos	Control de Accesos	Implementación de procedimiento específico y completo para el control de accesos
Gestión	PA-017	Evaluación de Riesgos	Cuentas de usuario	Actualizar y mejorar el procedimiento para cuentas de usuario orientándolo hacia la seguridad de la información
Gestión	PA-006	Evaluación de Riesgos	Campañas de concientización	Implementar plan de campañas para concientizar a los usuarios sobre seguridad
Gestión	PA-011	Evaluación de Riesgos	Continuidad del negocio	Actualización de política de continuidad del negocio y gestión de riesgos
Técnico	PA-012	Evaluación de Riesgos	Control de Accesos Físicos	Actualizar procedimientos de control de ingreso físico orienándolos hacia la seguridad de lainformación
Técnico	PA-013	Evaluación de Riesgos	Revision de funcionamiento de BDD	Implementar procedimiento para revisión de configuraciones y simulacros de funcionamiento de BDD
Técnico	PA-015	Evaluación de Riesgos	Autenticación de usuarios	Actualización de procedimiento para cuentas de usuario, incluyendo nuevos métodos de autenticación con múltiple factor de autenticación
Gestión	PA-016	Evaluación de Riesgos	Gestión de servicios de red	Implementar política para regular y controlar la gestion del servicio de red por parte del proveedor
Gestión	PA-018	Evaluación de Riesgos	Seguridad Tecnológica	Actualizar procedimiento para seguridad tecnológica, orientándolo a seguridad de la información, utilizar criterio del menor privilegio
Gestión	PA-019	Evaluación de Riesgos	Privilegios de usuarios	Implementación de procedimiento y controles de revisión continua de privilegios de usuarios
Gestión	PA-020	Evaluación de Riesgos	Gestión de contraseñas	Actualizar procedimientos e incluir política sobre uso de contraseñas predeterminadas
Gestión	PA-001	Evaluación de Riesgos	Capacitación	Implementación de un procedimiento de de capacitación permanente
Gestión	PA-002-a	Evaluación de Riesgos	Contratación	Mejora de procedimiento de contratación
Gestión	PA-002-b	Evaluación de Riesgos	Evaluación de desempeño	Implementación de procedimiento de Evaluación de desempeño
Gestión	PA-008	Evaluación de Riesgos	Auditoría interna	Revisar y actualizar procedimientos de auditoría interna y orientarlos hacia seguridad de la información
Técnico	PA-014	Evaluación de Riesgos	DLP	Implementación de DLP y procedimiento para el monitoreo del DLP
Técnico	PA-021	Evaluación de Riesgos	Control de datos	Implementar procedimiento específico para el control sobre los datos de entrada y salida
Gestión	PA-022	Evaluación de Riesgos	Integración	Implementar campañas de motivación e integración del personal regulares
Gestión	PA-024	Evaluación de Riesgos	Sanciones	Actualizar sanciones de reglamento interno orientadas a eventos de seguridad de la información
Gestión	PA-023	Evaluación de Riesgos	Convenios de confidencialidad	Actualizar convenios de confidencialidad con criterios de seguridad de la infromación

Figura 19. Modelo Operacional - 1

Metricas	Fecha Inicio	Fecha Fin	Responsable	Presupuesto	Estado
Número de días que han sido validadas las bases de datos	01/11/2021	30/12/2021	Jefe de TI	$ 1.000,00	Pendiente
Frecuencia de revisión de roles y responsabilidades asignadas	01/11/2021	30/11/2021	Riesgos	$ -	Pendiente
Porcentaje de completitud de implementación de directorio	01/11/2021	30/11/2021	Infraestructura	$ 1.000,00	Pendiente
Porcentaje de cumplimiento de controles de BDD	01/12/2021	30/12/2021	Jefe de TI	$ -	Pendiente
Porcentaje de cumplimiento de revisiones mensuales de equipos y usuarios	03/01/2022	31/01/2022	Jefe de TI	$ -	Pendiente
Número de dias que han sido revisados los logs de base de datos	03/01/2022	31/01/2022	Jefe de TI	$ -	Pendiente
Porcentaje de eventos de violación de accesos registrados	01/02/2022	28/02/2022	Jefe de TI	$ -	Pendiente
Porcentaje de cumplimiento de cambios periódicos de contraseñas	01/02/2022	28/02/2022	Jefe de TI	$ -	Pendiente
Porcentaje de cumplimiento de campañas de concientización de usuarios	01/03/2022	31/03/2022	Riesgos	$ 1.000,00	Pendiente
Porcentaje de sistemas de información que han realizado pruebas de planes de contingencia	01/03/2022	31/03/2022	Riesgos	$ 1.000,00	Pendiente
Porcentaje de autorización de accesos físicos	01/04/2022	29/04/2022	Seguridad Física	$ -	Pendiente
Porcentaje de cumplimiento de simulacros de funcionamiento de BDD	01/04/2022	29/04/2022	Jefe de TI	$ -	Pendiente
Porcentaje de usuarios con multiple factor de autenticación	02/05/2022	31/05/2022	Jefe de TI	$ 2.000,00	Pendiente
Porcentaje de eventos adversos en servicios de red	02/05/2022	31/05/2022	Jefe de TI	$ -	Pendiente
Porcentaje de eventos registrados de descarga de software no autorizado	01/06/2022	30/06/2022	Jefe de TI	$ -	Pendiente
Porcentaje de privilegios de usuarios revisados y controlados	01/06/2022	30/06/2022	Riesgos	$ -	Pendiente
Porcentaje de dispositivos cambiados contraseñas por deafult	01/07/2022	29/07/2022	Jefe de TI	$ -	Pendiente
Porcentaje de cumplimiento de planes de capacitación	01/07/2022	29/07/2022	RRHH	$ -	Pendiente
Nivel de rotación del personal	01/08/2022	31/08/2022	RRHH	$ -	Pendiente
Número de incidentes desantendidos	01/08/2022	31/08/2022	RRHH	$ -	Pendiente
Porcentaje de cumplimiento de auditorías	01/08/2022	31/08/2022	Riesgos	$ -	Pendiente
Número de eventos detectados por DLP	01/04/2022	31/10/2022	Jefe de TI	$ 5.000,00	Pendiente
Porcentaje de eventos registrados y notificados	01/09/2022	30/09/2022	Riesgos	$ -	Pendiente
Número de campañas de motivación e integración efectuadas	01/09/2022	30/09/2022	RRHH	$ 3.000,00	Pendiente
Número de sanciones levantadas por infracción de políticas de seguridad de la información	03/10/2022	31/10/2022	RRHH	$ -	Pendiente
Porcentaje de personas con acuerdos de confidencialidad actualizados	03/10/2022	31/10/2022	Logística	$ -	Pendiente

Figura 20. Modelo Operacional - 2

3. CONCLUSIONES

Existen activos de información de la organización que son de mucha importancia, tanto por la información que procesan como por el servicio que prestan y es necesario asegurarlas para garantizar la continuidad del negocio.

La carencia de un Sistema de Gestión de Seguridad de la información, en la actualidad, es dejar desprotegida, vulnerable a una organización ante los diferentes riesgos que pueden materializarse y que pueden ocasionar la destrucción de una empresa, aquí nace la importancia de su implementación.

La información almacenada y procesada acerca de los códigos aleatorios o códigos estáticos de las cerraduras electrónicas que la organización opera, para brindar un servicio seguro a sus clientes, deben ser tratadas con la importancia del caso, y se deben establecer todos los controles que garanticen que el servicio que se brinda con su operación, este disponible en el momento preciso, que su integridad no haya sido alterada y que su confidencialidad no haya sido violada.

El establecer el Sistema de Gestión de Seguridad de la información, brindará a la organización un esquema seguro de trabajo, un esquema seguro de operación y apoyará estratégicamente en la consecución de sus objetivos y en el crecimiento organizacional.

Todo cambio genera resistencia, por lo tanto, es muy importante que se capacite al personal y que se generen las campañas de concienciación necesarias, para que todos los colaboradores, conozcan y tengan claro la importancia de alinearse y cumplir con las políticas y procedimientos que el sistema establezca, teniendo

siempre en mente el riesgo que la actividad tiene, y, sobre todo, viviendo el día a día la cultura de prevención que la dirección tiene como prioridad.

4. REFERENCIAS

ISO 27001. (s.f.). Obtenido de https://normaiso27001.es/

ANEXOS