FACULTAD DE POSGRADOS

DESARROLLO DEL PROGRAMA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA IMPORTADORA DE VEHICULOS LTDA.

AUTOR

Alberto Carlos Santana Barrionuevo

AÑO

2021

FACULTAD DE POSGRADOS

DESARROLLO DEL PROGRAMA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA IMPORTADORA DE VEHICULOS LTDA.

Trabajo de titulación presentado en conformidad con los requisitos establecidos para optar por el título de Magister en Gestión de Seguridad de la Información

Autor:

Alberto Carlos Santana Barrionuevo.

Año

2021

AGRADECIMIENTOS

Yo; Alberto Carlos Santana Barrionuevo, quiero agradecer de a mi madre ya que con su apoyo en mis estudios y sus enseñanzas inculcadas hacia mi persona dieron como resultado la consecución de este proyecto.

A mi amada esposa quien con su apoyo incondicional y su impulso fue parte importante de la culminación de este proyecto.

Alberto S.

DEDICATORIA

Este proyecto está dedicado a mi madre y mi abuelo, quienes fueron artífices de inculcar en mi persona valores como la honestidad y el respeto, que dieron como resultado la finalización de este proyecto.

A mi amada esposa Mélida, quien ha sido el motor de apoyo desde siempre.

A mi primo Alex que con sus consejos y apoyo continuo permitieron sea posible la realización de este proyecto.

Alberto S.

RESUMEN

El presente documento detalla el desarrollo de un sistema de Gestión de Seguridad de la Información para la Importadora de Vehículos Ltda., capaz de garantizar los principios de confidencialidad, integridad y disponibilidad de la información de sus activos y sus sistemas.

Este Sistema se desarrolló, conforme a los lineamientos de los marcos de referencia como: ISO (*Internacional Standard Organization*) 27001, 27002, NIST (*National Institute Of Standards And Technology*), Maragerit y COBIT en su versión 5 entre otros, acorde a los fundamentos teóricos y las buenas prácticas en ellos descritos para los diferentes escenarios.

Por medio del desarrollo del SGSI se realizará un Diagnóstico de la organización basado en NIST e ISO 27001, el mismo que arrojará un resultado del estado actual de la organización y sus falencias, posterior a ello se realizará un análisis del activo más crítico de la organización previa la clasificación de la información que procesa y sus riesgos, para finalmente proponer el programa con los planes de acción a realizarse y sus mejoras continuas.

En base al análisis efectuado y la respectiva documentación generada, la organización y el Gerente de Tecnología podrá asegurar la información que maneja la empresa y hacer frente a posibles eventos de seguridad que se presenten a lo largo del tiempo, teniendo ya un Sistema de Gestión de Seguridad de la Información ajustado a la realidad de la Organización.

El Sistema de Gestión de Seguridad de la Información, al estar alineado a varios marcos de referencia, permite su mejora continua y su evaluación periódica, permitiéndole estar actualizado de manera constante.

ABSTRACT

This document details the development of an Information Security Management system for Importer of Vehicles Ltda. Capable of guaranteeing the principles of confidentiality, integrity, and availability of information on its assets and its systems.

This System was developed, in accordance with the guidelines of the reference frameworks such as: ISO (International Standard Organization) 27001, 27002, NIST (National Institute Of Standards And Technology), Maragerit and COBIT in version 5 among others, according to the fundamentals theoretical and good practices described in them for the different scenarios.

Through the development of the ISMS, a Diagnosis of the organization based on NIST and ISO 27001 will be carried out, which will give a result of the current state of the organization and its shortcomings, after which an analysis of the most critical asset of the organization will be carried out. after classifying the information, it processes and its risks, to finally propose the program with the action plans to be carried out and its continuous improvements.

Based on the analysis carried out and the respective documentation generated, the organization and the Technology Manager will be able to secure the information handled by the company and deal with possible security events that may arise over time, already having a Management System of Information Security adjusted to the reality of the Organization.

The Information Security Management System, being aligned to various reference frameworks, allows its continuous improvement and periodic evaluation, allowing it to be constantly updated.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1. INTRODUCCIÓN

El siguiente trabajo consiste en proveer a la Importadora de Vehículos Ltda. un Sistema de Gestión de Seguridad de la Información, que le permita garantizar la confidencialidad, integridad y disponibilidad de la información que maneja.

1.1 Antecedentes

Importadora de vehículos Ltda. es una empresa que se dedica a la importación de vehículos de alta gama de procedencia asiática, distribuyéndolos a diferentes concesionarios.

Como objetivo principal la empresa se dedica a importar vehículos de calidad y garantía, satisfaciendo de esta manera al creciente mercado automotriz.

Su visión está alineada a convertirse en el líder de distribución de vehículos asiáticos.

Adicional a la importación, las tareas principales, se alinean a los requerimientos de mercadeo indicados por el fabricante y la gestión de logística del producto.

Dentro de la empresa la estrategia organizacional, las alianzas con organizaciones locales y la orientación al cliente, definen un camino a seguir. En el cual la oferta de valor gira en torno al excelente producto ofertado y los clientes satisfechos.

Todo esto dentro del marco legal y normativa vigente tanto en el territorio nacional, como en el de procedencia de los automotores.

1.2 Objetivo General

Desarrollar un Sistema de Gestión de Seguridad de la Información para la Importadora de Vehículos Ltda.

1.3 Objetivos específicos

- Realizar un diagnóstico de la organización según el modelo operacional definido.
- Clasificación e inventario los activos de información definiendo los críticos para la organización.
- Desarrollo de Políticas de Alto nivel alineados al marco de referencia

ISO 27001.

- Realizar un análisis de amenazas y vulnerabilidades de activos de información críticos.

1.4 Alcance

El presente Sistema de Gestión de Seguridad de la Información se desarrolla para la Importadora de Vehículos Ltda., la misma que consta de las siguientes fases.

Figura 1. Alcance del Proyecto SGSI

Tomado de (Juan Carlos López, 2021).

1.5 Descripción de la Problemática

Actualmente la organización, no cuenta con un proceso formal o políticas propias referentes a seguridad de la información, lo cual la hace vulnerable y susceptible a robo, fuga y secuestro de su información.

Al ser el área de tecnologías de la información un área de apoyo clave, no cuentan con un manejo formal de políticas de seguridad de la información, que se encuentren documentadas, o alineadas a un marco de referencia.

Algunos procesos informales que se manejan han sido heredados o tomados de la alianza que se tiene con las organizaciones asociadas.

Dentro de estos se pueden mencionar los siguientes:

- Creación de usuarios ERP y servicios *cloud*,
- Confidencialidad y uso de datos, y;
- Uso de servicios de telecomunicaciones y redes.

Para mitigar la problemática descrita con anterioridad, se plantea el desarrollo de un Sistema de Gestión de Seguridad de la Información para Importadora de Vehículos Ltda., basándose en marcos de referencia y estándares, que garanticen una gestión adecuada, eficiente, documentada y controlada para la operación diaria de la organización, priorizando los principios de privacidad, confidencialidad, integridad y disponibilidad de la información.

El desarrollo del SGSI permitirá realizar un mejor análisis personalizado de la situación actual de la organización y sus oportunidades de mejora. Realizando un programa desde cero sin ajustar un conjunto de políticas derivadas de otras organizaciones, que posiblemente no se ajusten a la realidad de esta.

1.6 Beneficios de la Implementación de un SGSI

- Reduce el riesgo de pérdida y robo de información,
- Disminuye el impacto ante eventos de seguridad y/o ataques contra la empresa,
- Establece una metodología para gestionar la seguridad de la información y sus planes de acción para mitigar las amenazas,
- Permite medir y evaluar de manera continua el riesgo, y;
- Permite a la organización ser resiliente ante eventos catastróficos de seguridad.

2. DESARROLLO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

2.1 Evaluación del Estado actual

El principal objetivo del sistema de gestión de seguridad de la Información para la compañía Importadora de vehículos Ltda. Es proporcionar integridad, disponibilidad y confidencialidad a la información tratada por parte de la organización.

Este análisis busca mostrar de manera sistémica y ordenada el estado actual de la organización, alineado a los marcos de referencia y buenas prácticas, escogidos para su evaluación.

El marco de referencia utilizado para la evaluación de la situación actual de la empresa es NIST, adicional a este, también se tomó ISO27001-27002 y algunos puntos de COBIT 5.

Los valores agrupados por categoría nos permiten identificar los puntos más débiles a nivel macro, en los cuales es necesaria la mejora o su implementación total.

Los valores utilizados y considerados para este análisis son los que se muestran en la Tabla 1

Tabla 1. Ponderación.

Descripción	Valor
Nulo	0
Bajo	5
Medio	10
Alto	20

2.1.1 Resultados de la Evaluación

Como resultado resumido en las categorías indicadas por NIST tenemos lo descrito en la Tabla 2, el análisis detallado se describe en el Anexo A.

Tabla 2. Resumen Ponderación por Función y Categoría

Función	Categoría	Total
IDENTIFICAR (ID)	Gestión de activos (ID.AM)	4.17
	Entorno empresarial (ID.BE)	7.00
	Gobernanza (ID.GV)	1.25
	Evaluación de riesgos (ID.RA)	1.67
	Estrategia de gestión de riesgos (ID.RM)	5.00
	Gestión del riesgo de la cadena de suministro (ID.SC)	0.00
PROTEGER (PR)	Gestión de identidad, autenticación y control de acceso (PR.AC)	4.29
	Concienciación y capacitación (PR.AT)	6.00
	Seguridad de los datos (PR.DS)	7.50
	Procesos y procedimientos de protección de la información (PR.IP)	1.67
	Mantenimiento (PR.MA)	5.00
	Tecnología de protección (PR.PT)	3.00
DETECTAR (DE)	Anomalías y Eventos (DE.AE)	1.00
	Monitoreo Continuo de la Seguridad (DE.CM)	1.88
	Procesos de Detección (DE.DP)	2.00
RESPONDER (RS)	Planificación de la Respuesta (RS.RP)	0.00
	Comunicaciones (RS.CO)	2.00
	Análisis (RS.AN)	0.00
	Mitigación (RS.MI)	1.67
	Mejoras (RS.IM)	0.00
RECUPERAR (RC)	Planificación de la recuperación (RC.RP)	0.00
	Mejoras (RC.IM)	0.00
	Comunicaciones (RC.CO)	0.00
Total, general		**2.78**

Adaptado de (National Institute of Standards and Technology, 2018)

Figura 2. Resumen Ponderación Por Categoría

Los resultados del análisis realizado son alarmantes, ya que da una muestra de que la organización no cuenta con los procesos necesarios, que puedan hacer frente a eventos de seguridad de la información.

2.1.2 Hallazgos

Como se puede visualizar en la gráfica en su mayoría los valores están en un nivel entre bajo y medio, llegando en algunos casos a nulo, dando a conocer las debilidades y falencias que existen actualmente.

Los principales hallazgos encontrados según la gráfica anterior son los de tallados en la Tabla 3:

Tabla 3. Hallazgos críticos

Función	Categoría	Promedio Por Categoría	Hallazgo Critico	Conclusión de Hallazgo
IDENTIFICAR(ID)	Gobernanza (ID.GV)	1.25	Si	No tienen políticas definidas para seguridad de la información
	Evaluación de riesgos (ID.RA)	1.67	Si	Ausencia de procesos para determinar amenazas y vulnerabilidades
	Gestión del riesgo de la cadena de suministro (ID.SC)	0.00	Si	No tiene un proceso para gestionar los riesgos de seguridad de la información
PROTEGER(PR)	Procesos y procedimientos de protección de la información (PR.IP)	1.67	Si	No cuenta con un proceso de protección de la información.
DETECTAR (DE)	Anomalías y Eventos (DE.AE)	1.00	Si	No cuenta con procedimientos de detección adecuados y definidos.
	Monitoreo Continuo de la Seguridad (DE.CM)	1.88	Si	Ausencia de herramientas especializadas de monitoreo de entorno y comunicaciones
RESPONDER (RS)	Planificación de la Respuesta (RS.RP)	0.00	Si	No posee un plan de respuesta
	Análisis (RS.AN)	0.00	Si	No posee un plan de manejo de incidentes
	Mitigación (RS.MI)	1.67	Si	Ausencia de un plan formal de contingencia
	Mejoras (RS.IM)	0.00	Si	No cuenta con una base de conocimientos que permita mitigar los incidentes de seguridad
RECUPERAR (RC)	Planificación de la recuperación (RC.RP)	0.00	Si	No cuenta con un plan de resiliencia

	Mejoras (RC.IM)	0.00	Si	No cuenta con un plan de recuperación
	Comunicaciones (RC.CO)	0.00	Si	No cuenta con un plan de mitigación del impacto de posibles eventos de seguridad de la información.

Adaptado de (National Institute of Standards and Technology, 2018)

Si bien es cierto hasta el momento no ha existido un evento de seguridad que haya comprometido la información de la organización, con este análisis muestra una clara idea de lo vulnerable que se encuentra.

2.2 Desarrollo de Políticas

Para el desarrollo de políticas se tomó como marco de referencia ISO 27001 e ISO 27002 (ISO (Internacional Organization for Standardization), 2013).

Esta política establece requisitos para la adhesión de buenas prácticas de seguridad de la información en el uso de sistemas y comunicaciones en la Importadora de Vehículos Ltda.

2.2.1 Alcance de la Política

La política descrita, será aplicable a todos los usuarios de la organización, incluyendo empleados, contratistas y proveedores que actúen en nombre de la empresa y tengan acceso a la información. También es aplicable a los activos de información propios de la institución y aquellos que se utilicen dentro de las instalaciones, y/o hagan uso de los recursos de red de la organización.

2.2.2 Objetivo General de la Política

Todos los usuarios que utilicen los sistemas de la empresa son responsables de proteger los recursos corporativos y la información procesada, almacenada o transmitida, como se establece en esta política. La cual tiene como objetivo determinar una cultura de seguridad de la información en la organización. Esta política abarca todas las directrices y procesos necesarios para proteger la información y los activos de información, alineándose a los principios de confidencialidad, integridad y disponibilidad.

2.2.3 Objetivos Específicos de la Política

Con el fin de proteger la información y los activos de información de la Importadora de Vehículos Ltda, se han desarrollado controles, cuyos objetivos son los siguientes:

- Apoyar la operación,
- Proteger el negocio, y;
- Promover una conducta adecuada de seguridad de la información.

Toda la información almacenada, transmitida y procesada por los sistemas corporativos, es de propiedad exclusiva de la importadora de vehículos, sin tomar en cuenta su contenido.

2.2.4 Políticas

1. Esta política deberá ser revisada de manera periódica en periodos de tiempo planificados, con el fin de asegurar su idoneidad, adecuación y eficacia continua.
2. Todos los activos de información deberán tener asignados un propietario, así como sus funciones y responsabilidades de protección de la información.
3. Los activos de información deben ser debidamente inventariados y clasificados, tomando en cuenta su valor, privacidad y confidencialidad.
4. Se debe cumplir el proceso de etiquetado de la información definido por la organización, tanto en archivos físicos como digitales.
5. Se debe implementar y cumplir un procedimiento para el manejo y gestión de medios de soporte removibles.
6. Los medios de soporte físico serán asignados a un responsable, quien será custodio de los mismos y los protegerá del acceso no autorizado, ya sea durante su permanencia o transporte.

7. Se deben definir roles y asignar los responsables de seguridad de la información.
8. Se debe segregar las funciones de cada área específica, para reducir la posible modificación no autorizada o no intencional de la información, conflicto de intereses o el uso indebido de las mismas.
9. No se debe aislar la seguridad de la información por el tipo de proyecto, esta debe ser considerada en cualquier proyecto, ya sea interno o externo.
10. Adoptar medidas de seguridad en el uso de dispositivos portátiles y móviles que almacenen, transmitan y realicen procesamiento de información de la compañía.
11. Se deberá asegurar los lugares físicos de procesamiento, almacenamiento de información y comunicaciones, con controles apropiados, para proteger contra el acceso no autorizado o ilegal a estos.
12. Establecer medidas de protección de la información que se accede, procesa o almacena en los lugares destinados al teletrabajo.
13. La dirección deberá exigir a todos los empleados y contratistas o proveedores la aplicación de la seguridad de la información, alineadas a las políticas y procedimientos de la organización.
14. Se implementarán de manera frecuente planes de concientización y formación del personal en conocimientos y lineamientos básicos de seguridad y tratamiento de la información.
15. Todos los empleados de manera obligatoria deberán asistir a los entrenamientos periódicos organizados por la compañía, con el fin de reforzar y crear una cultura de seguridad de la información.
16. Todo empleado que haya cometido una violación a la seguridad de la información será sometido a un proceso disciplinario formal.

17. Las responsabilidades y deberes de seguridad de la información permanecerán válidos, inclusive posterior a la terminación de las relaciones laborales o cambio de responsabilidades.
18. Todos los empleados, usuarios y grupos de interés, deberán devolver todos los activos de la organización que se encuentren a su cargo.
19. Se establecerán procedimientos y una base de conocimientos documentados para identificar incidentes en tecnología de la información.
20. Se deberá documentar el proceso operativo, el cual deberá estar a disposición de todos los usuarios que lo necesiten.
21. Se deberá seguir un proceso de gestión de cambios en las instalaciones y sistemas de procesamiento de información
22. Los entornos de producción y pruebas de los sistemas de información estarán debidamente separados y se realizará control de accesos a los mismos.
23. Se deberá mantener una gestión de aplicaciones que permita aplicar pruebas de seguridad a los sistemas y herramientas destinadas para el procesamiento de información.
24. Se deberá contar con mecanismos de protección ante código malicioso o virus informáticos que permitan la detección, prevención y recuperación ante eventos de seguridad de la información.
25. Se deberá seguir un procedimiento adecuado para generación y test de copias de seguridad de la información, software e imágenes de los sistemas.
26. Se verá llevar una gestión de registro de eventos, los cuales deben ser conservados y revisados frecuentemente.

27. Los sistemas de procesamiento de información deberán estar sincronizados sus relojes para evitar que la integridad de la información que procesan sea comprometida.
28. Se deberá seguir un procedimiento de instalación de sistemas operativos, guardando un orden especifico e inventariando sus licencias.
29. Se deberá realizar una revisión periódica de vulnerabilidades de los sistemas en un ambiente controlado, que permita mitigar y tomar acciones ante posibles o nuevas vulnerabilidades.
30. Se restringe la instalación de software no autorizado por la organización, especialmente las aplicaciones que no tengan relación con el giro del negocio y no hayan sido notificadas al departamento de tecnología.
31. Se debe realizar un control y autenticación de uso de redes de información, garantizando la transmisión y transporte de la información de la empresa.
32. Se debe segmentar los recursos de red, entre usuarios y sistemas de información.
33. Se deberá establecer acuerdos sobre la transferencia de información entre la organización y partes externas o proveedores.
34. Se deberá asegurar y proteger el uso de servicios y aplicaciones de la organización que deban pasar por redes públicas.
35. El control de cuentas y usuarios se realizará en conjunto y coordinación con talento humano, estando sujetos todos los empleados al cumplimiento de la política de seguridad de la información.
36. Se establecerá el uso de técnicas adecuadas de autenticación y autorización, para el acceso de usuarios a los sistemas de información y recursos tecnológicos corporativos.

37. Se restringirá y controlará la asignación y uso de derechos de acceso privilegiados.
38. La asignación de información de autenticación secreta será controlada por un proceso de gestión formal.
39. Los propietarios de los activos de información realizarán una revisión periódica de acceso de los usuarios en periodos de tiempo regulares.
40. Las cuentas y derechos de acceso deberán ser canceladas o suspendidas a la terminación de las relaciones laborales, del contrato de servicios o acuerdos.
41. Se exigirá a los colaboradores el cumplimiento de prácticas de la organización definidas para el uso de información de autenticación secreta.
42. El acceso a la información y funciones están definidos y serán asignados de acuerdo con el rol del colaborador.
43. Para el acceso a los sistemas de información se deberá utilizar un procedimiento de conexión segura.
44. Los programas o software utilitario que pudiesen anular las capacidades del sistema o sus controles serán restringidos.
45. En caso de que existiese un desarrollo de software propietario, el acceso a su código fuente estará restringido únicamente al personal autorizado para su uso o modificación.
46. Se deberá asegurar los ambientes de desarrollo.
47. La empresa deberá supervisar y realizar las respectivas revisiones y validaciones del software desarrollado por terceros.
48. Se deberá asegurar la existencia de métodos criptográficos para la protección de la información, así como su control, continua revisión de claves y tiempo de vida mientras se encuentran vigentes.

49. Los sitios de procesamiento de información deberán estar aislados para evitar el acceso no autorizado.
50. La ubicación de equipos deberán ser lugares que reduzcan el riesgo de amenazas y peligros ambientales.
51. Los equipos deberán ser protegidos ante fallas de interrupciones de energía o anomalías en ellas.
52. El cableado de energía y de telecomunicaciones que permite el transporte de datos deberán ser protegidos contra intercepciones intencionales y no intencionales.
53. Los equipos e infraestructura activa deberán recibir mantenimiento según su función y operatividad en periodos de tiempo planificados.
54. Se deberá asegurar los equipos que se encuentren operando fuera del predio de la organización.
55. Se deberán realizar copias de seguridad de los sistemas esenciales para el giro de negocio o que procesen información de la corporación, asegurando su almacenamiento y el acceso a este.
56. Se deberá contar con la redundancia suficiente en las instalaciones y servicios que permitan cumplir con los requisitos de disponibilidad.
57. Se establecerá un proceso de borrado y eliminación de información, así como la correcta destrucción de los medios en los cuales se almacena.
58. Se deberá establecer el tratamiento de la seguridad de la información dentro de los acuerdos establecidos con los proveedores.
59. Se deberá realizar seguimiento y auditar los servicios de los proveedores con el fin de verificar el cumplimiento de políticas y métodos que aseguren y garanticen la seguridad de la información.

60. Se debe gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido mejora de servicios, cambio de políticas y controles de seguridad de la información.

61. Las prácticas de seguridad de la información serán revisadas y auditadas regularmente, para verificar su cumplimiento.

62. Se debe delegar un responsable portavoz de informar los eventos de seguridad de la información, el cual será el encargado de comunicar a través de los canales oficiales para el efecto.

63. Los empleados, proveedores, contratistas o cualquier persona o grupo de interés, que detecte u observe alguna debilidad de seguridad de la información, deberá informarla a la brevedad posible.

64. Se deberá realizar una evaluación constante de eventos de seguridad.

65. Los procesos de negocio y deberán alinearse a las políticas descritas en este documento.

66. Se deberá implementar un plan de gestión de la continuidad, para mitigar el impacto de interrupciones causadas por desastres naturales o eventos de seguridad.

67. Se debe identificar, documentar y mantener actualizados explícitamente todos los requisitos legislativos estatuarios, reglamentarios y contractuales pertinentes.

68. Se debe establecer y acatar procedimientos de derechos de propiedad intelectual tanto para el cumplimiento de los requisitos legislativos y de reglamentación contractuales, como para el correcto uso de productos de software o hardware licenciados.

69. Se deberá asegurar la privacidad y proteger la información identificable, como se exige en la legislación y normativa descrita en la ley organiza de protección de datos personales.

70. Se deberá contar con una revisión independiente de la seguridad de la información, que incluye, políticas, controles, procesos y procedimientos.

71. Se deberá cumplir con una revisión técnica periódica de los sistemas de procesamiento y almacenamiento de información, para verificar el cumplimiento de la política y las normativas.

2.3 Métricas

Considerando el modelo operacional definido en base a NIST, para métricas se consideró el marco de referencia COBIT5 acorde a las categorías y subcategorías de NIST como se muestra en la Tabla 4, lo cual se detalla en el Anexo B.

Tabla 4. Categorías NIST vs COBIT5.

Función	Categoría	Puntuación	Cobit 5
IDENTIFICAR (ID)	Gestión de activos (ID.AM)	4.17	BAI09.01, BAI09.02, BAI09.05, DSS05.02, APO02.02, APO10.04, DSS01.02, APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02, APO01.02, APO07.06, APO13.01, DSS06.03
	Entorno empresarial (ID.BE)	7.00	APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05, APO02.06, APO03.01, APO02.01, APO10.01, BAI04.02, BAI09.02, BAI03.02, DSS04.02
	Gobernanza (ID. GV)	1.25	APO01.03, APO13.01, EDM01.01, EDM01.02, APO01.02, APO10.03, APO13.02, DSS05.04, BAI02.01, MEA03.01, MEA03.04, EDM03.02, APO12.02, APO12.05, DSS04.02
	Evaluación de riesgos (ID.RA)	1.67	APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02, BAI08.01, DSS04.02, APO12.05, APO13.02

	Estrategia de gestión de riesgos (ID.RM)	5.00	APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02, APO12.06, APO12.02
	Gestión del riesgo de la cadena de suministro (ID.SC)	0.00	APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02, APO10.02, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.06, APO10.03, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05, DSS04.04
	Gestión de identidad, autenticación y control de acceso (PR.AC)	4.29	DSS05.04, DSS06.03, DSS01.04, DSS05.05, APO13.01, DSS01.04, DSS05.03, DSS01.05, DSS05.02, DSS05.07, DSS06.03
	Concienciación y capacitación (PR.AT)	6.00	APO07.03, BAI05.07, APO07.02, DSS05.04, DSS06.03, APO07.03, APO07.06, APO10.04, APO10.05, EDM01.01, APO01.02
	Seguridad de los datos (PR.DS)	7.50	APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06, DSS05.02, BAI09.03, APO13.01, BAI04.04, DSS05.04, DSS05.07, DSS06.02, BAI03.08, BAI07.04, BAI03.05

	Procesos y procedimientos de protección de la información (PR. IP)	1.67	BAI10.01, BAI10.02, BAI10.03, BAI10.05, APO13.01, BAI03.01, BAI03.02, BAI03.03, BAI01.06, BAI06.01, APO13.01, DSS01.01, DSS04.07, DSS01.04, DSS05.05, BAI09.03, DSS05.06, APO12.06, DSS04.05, BAI08.04, DSS03.04, DSS04.03, DSS04.04, APO07.01, APO07.02, APO07.03, APO07.04, APO07.05, BAI03.10, DSS05.01, DSS05.02
	Mantenimiento (PR.MA)	5.00	BAI03.10, BAI09.02, BAI09.03, DSS01.05, DSS05.04
	Tecnología de protección (PR.PT)	3.00	APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01, APO13.01, DSS05.02, DSS05.06, DSS05.02, DSS05.05, DSS06.06, DSS05.02, APO13.01, BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05
DETECTAR (DE)	Anomalías y Eventos (DE.AE)	1.00	DSS03.01, DSS05.07, BAI08.02, APO12.06
	Monitoreo Continuo de la Seguridad (DE.CM)	1.88	DSS01.03, DSS03.05, DSS05.07, DSS01.04, DSS01.05, DSS05.07, DSS05.01, APO07.06, APO10.05, DSS05.02, DSS05.05, BAI03.10, DSS05.01
	Procesos de Detección (DE. DP)	2.00	APO01.02, DSS05.01, DSS06.03, DSS06.01, MEA03.03, MEA03.04, APO13.02, DSS05.02, APO08.04, APO12.06, DSS02.05, DSS04.05
RESPONDER (RS)	Planificación de la Respuesta (RS.RP)	0.00	APO12.06
	Comunicaciones (RS.CO)	2.00	EDM03.02, APO01.02, APO12.03, DSS01.03, DSS03.04, BAI08.04

	Análisis (RS.AN)	0.00	DSS02.04, DSS02.07, DSS02.02, APO12.06, DSS03.02, DSS05.07, EDM03.02, DSS05.07
	Mitigación (RS.MI)	1.67	APO12.06
	Mejoras (RS.IM)	0.00	DSS04.08
RECUPERAR (RC)	Planificación de la recuperación (RC.RP)	0.00	APO12.06, DSS02.05, DSS03.04
	Mejoras (RC.IM)	0.00	APO12.06, BAI05.07, DSS04.08, BAI07.08
	Comunicaciones (RC.CO)	0.00	EDM03.02, MEA03.02, APO12.06

Adaptado de (National Institute of Standards and Technology, 2018)

2.4 Tipos de Información y Activos Críticos

Como parte del desarrollo del Programa de seguridad de la información, se determinó y registro el tipo de información que maneja el proceso de importación de vehículos y los activos que tratan o almacenan esta información, adicional a ello también se tomó en cuenta el sistema de nómina de empleados, debido a la sensibilidad de los datos que contiene.

2.4.1 Apetito al Riesgo e Impacto

Como modulador de apetito y valoración de Impacto se consideró como referencia las tablas y cuadros de calor descritos en el Anexo C.

Para la clasificación e inventario de activos se tomó en cuenta tres entidades fundamentales del proceso como son:

- Proveedores,
- Empleados, y;
- Clientes.

Dentro de ellas se determinaron los tipos de información de acuerdo con la siguiente tabla:

Tabla 5. Entidades y Tipos de Información.

Entidad	Nombre del tipo de información	Tipo de Información
Proveedores	Modelos de Vehículos	Listado de Modelos y versiones de vehículos
	Inventario de Vehículos	Cantidad, Costo y Precio de vehículos
	Información Aduanera	Información Impuestos y aranceles aduaneros
	Información Legal	Contratos y Acuerdos de Importación Información Relacionada con Agente Aduanero
	Información Bancaria	Detalle de datos para transferencias bancarias al Exterior (Swift,IBAN, etc)
Empleados	Domicilio	Datos de dirección de domicilio y referencias
	Información Tributaria	Formulario 107, Impuesto a la Renta, RDEP(Anexo de relación de dependencia)
	Información Legal	Juicios de Alimentos Estatus Migratorio Antecedentes Penales Contratos Laborales
	Información Bancaria	Datos de cuentas bancarias para pago de nómina, utilidades y otros Beneficios de ley

	Datos personales	Ficha del empleado (Nombres, fecha de nacimiento, instrucción, Estado civil, Avisos de entrada y salida del Iess)
	Información Médica	Información de estado de salud del empleado (Enfermedades Existentes -Preexistentes, Exámenes Preocupaciones y Ocupacionales, Discapacidades o Sustitutos)
	Laborales	Currículo Laboral del empleado (Salario, Cargo, jefe inmediato, Referencias Laborales, Historial Laboral)
Clientes	Datos de Facturación	Datos de contactabilidad (Identificación, dirección, teléfonos, correo electrónico, contactos)
	Información Tributaria	Información relacionada para emisión de retenciones (Tipo de Contribuyente)
	Información Unidad de Análisis Financiero (UAFE)	Formularios UAFE Conozca su Cliente
	Información Bancaria	Datos bancarios para devoluciones y rebates
	Información Dealer	Datos de entrega Contactos y direcciones de Entrega
	Información de Marketing	Información de Campañas Publicitarias y Presentaciones de la Marca
	Información de Exonerados	Datos sensibles de Clientes con Capacidades Especiales (Solicitudes, Certificados)

Posterior a ello se analizó y evaluó la criticidad de la información en base a la integridad, disponibilidad y confidencialidad, su probabilidad de ocurrencia y el

impacto, cuyo resultado se consideró la mayor valoración de ellos, lo cual se describe a detalle en el Anexo C.

2.4.2 Resumen de Activos Críticos

De acuerdo con el análisis de la criticidad de activos indicados en el Anexo C, se tiene el resumen indicado en la Tabla 6:

Tabla 6. Resumen de Activos Críticos.

Activo de Información	Hits máximo Nivel de Criticidad
Unidad NAS(SYNOLOGY)	2
Base de Datos ERP (SQL SERVER 2017)	3
BDD Sistema de gestión de nómina (SQL SERVER 2014)	2
Anaqueles Físicos de Archivo	1
Nube Privada (ONEDRIVE)	2

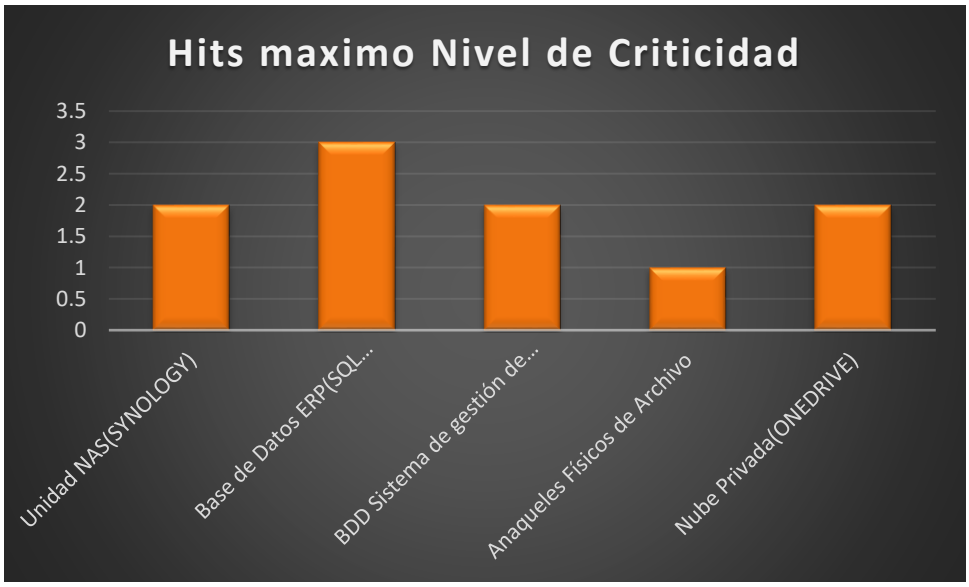


Figura 3. Activos de Mayor Criticidad

En el gráfico se puede evidenciar que el activo con mayor nivel de criticidad y uso es la base de datos.

2.4 Evaluación de Riegos del Activo Critico

Basándonos en el análisis realizado en el punto anterior, se toma como activo de análisis la base de datos, la cual se analiza en base al marco de referencia Margerit – versión 3.0.

Dentro de la siguiente tabla se muestran las principales amenazas para el tipo de activo Datos de Información con sus respectivas dimensiones:

Tabla 7. Amenazas y Dimensiones para Activo de Información.

Categoría	Amenazas	Dimensiones
[E] Errores y fallos no intencionados	[E.1] Errores de los usuarios	I C D
	[E.2] Errores del administrador	D I C
	[E.15] Alteración accidental de la información	I
	[E.18] Destrucción de información	D
	[E.19] Fugas de información	C
[A] Ataques intencionados	[A.5] Suplantación de la identidad del usuario	C A I
	[A.6] Abuso de privilegios de acceso	C I D
	[A.11] Acceso no autorizado	C I
	[A.15] Modificación deliberada de la información	I
	[A.18] Destrucción de información	D
	[A.19] Divulgación de información	C

Tomado de (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012).

En donde C significa Confidencialidad, I Integridad, D disponibilidad y A Autenticidad.

Posterior a ello se evalúa el riesgo inherente que es el resultado de la probabilidad por el impacto, para posteriormente determinar el riesgo residual el cual es obtenido a partir del riesgo inherente menos los controles detallados y

encontrado para este activo de información, cuyo análisis se describe en el Anexo D, juntamente con el *roadmap* de acción para mitigar las vulnerabilidades encontradas.

2.5 Programa de SGSI

El programa para el SGSI que se muestra a continuación en la Tabla 8, el mismo que detalla los planes de acción definidos según el análisis realizado para la Importadora de Vehículos Ltda.

Tabla 8. Programa del Sistema de Seguridad de la Información de la Importadora de Vehículos Ltda.

ENTIDAD	CODIGO	PLAN DE ACCION	RESPONSABLE	ACCOUNTABLE	FECHA INICIO	FECHA FIN
DIAGNOSTICO del SGSI	DG-PAC-01	Realizar un análisis de riesgo con todos los actores de la infraestructura critica alineado a un marco de referencia.	Analista de Sistemas	Gerente de Tecnología	1/7/2021	10/8/2021
	DG-PAC-02	Definir políticas para la seguridad de la información	Analista de Sistemas	Gerente de Tecnología	1/8/2021	31/10/2021
	DG-PAC-03	Establecer política que regule el acceso a la auditoria y su divulgación.	Analista de Procesos	Gerente de Tecnología	1/8/2021	31/10/2021
	DG-PAC-04	Implementación de Política para uso de medios extraíbles que incluya un registro de eventos de trasferencia de información.	Analista de Sistemas	Gerente de Tecnología	1/8/2021	31/10/2021
	DG-PAC-05	Socializar e incorporar en las políticas, lineamientos de buenas prácticas de transferencia de información	Analista de Procesos	Gerente de Tecnología	1/8/2021	31/10/2021
	DG-PAC-06	Mejorar el inventario existente, detallando sus movimientos y actualizando sus responsables.	Analista de Infraestructura	Gerente de Tecnología	15/11/2021	20/11/2021
	DG-PAC-07	Establecer políticas formales de seguridad de la información	Analista de Sistemas	Gerente de Tecnología	15/11/2021	20/11/2021

	DG-PAC-08	Diseña e implementar políticas y procesos de intercambio y trasferencia de información.	Analista de Procesos	Gerente de Tecnología	22/11/2021	30/11/2021
	DG-PAC-09	Implementar un *Unified threat management* tomando en cuenta las necesidades de conectividad de la organización.	Analista de Infraestructura	Gerente de Tecnología	15/11/2021	30/11/2021
	DG-PAC-10	Implementar herramientas de monitoreo, realizar consultorías o *pentesting*	Analista de Infraestructura	Gerente de Tecnología	15/11/2021	30/11/2021
	DG-PAC-11	Complementar las herramientas de *endpoint* con: ips, dlp, políticas y formación de usuarios para prevención de incidentes relacionados con la seguridad.	Analista de Infraestructura	Gerente de Tecnología	15/11/2021	30/11/2021
	DG-PAC-12	Realizar pruebas de funcionalidad de herramientas de seguridad informatica.	Analista de Infraestructura	Gerente de Tecnología	15/11/2021	30/11/2021
	DG-PAC-13	Definir formal y detalladamente responsabilidades del tratamiento y seguridad de la información.	Analista de Sistemas	Gerente de Tecnología	1/12/2021	31/12/2021
	DG-PAC-14	Establecer políticas bien definidas de tratamiento de información con proveedores.	Analista de Sistemas	Gerente de Tecnología	15/11/2021	31/12/2021

	DG-PAC-15	Exigir a proveedores establecer sus responsabilidades referentes a seguridad de la información.	Analista de Sistemas	Gerente de Tecnología	1/12/2021	31/12/2021
	DG-PAC-16	Definir y documentar roles y responsabilidades referentes a seguridad de la información.	Analista de Sistemas	Gerente de Tecnología	23/12/2021	31/12/2021
	DG-PAC-17	Realizar asignación formal de roles y responsabilidades.	Analista de Sistemas	Gerente de Tecnología	23/12/2021	31/12/2021
	DG-PAC-18	Evaluación y definición de ciclo de vida de aplicaciones utilizadas con el proveedor de servicios y sistemas de información.	Analista de Sistemas	Gerente de Tecnología	15/11/2021	31/12/2021
	DG-PAC-19	Implementar herramientas de seguridad de equipos móviles.	Analista de Infraestructura	Gerente de Tecnología	1/12/2021	31/12/2021
	DG-PAC-20	Establecer una política de uso de dispositivos personales y el correcto uso de equipos corporativos.	Analista de Sistemas	Gerente de Tecnología	1/12/2021	31/12/2021
	DG-PAC-21	Definir factores externos e internos que afecten la seguridad de la información.	Analista de Sistemas	Gerente de Tecnología	3/1/2022	9/1/2022
	DG-PAC-22	Realizar seguimiento de uso de recursos y hacer una proyección de crecimiento futuro.	Analista de Procesos	Gerente de Tecnología	10/1/2022	16/1/2022

	DG-PAC-23	Realizar un análisis y definir un portafolio de gestión de riesgos	Analista de Sistemas	Gerente de Tecnología	17/1/2022	31/1/2022
	DG-PAC-24	Segmentación de red y protección de acceso.	Analista de Infraestructura	Gerente de Tecnología	15/11/2021	15/2/2022
	DG-PAC-25	Realizar una gestión de vulnerabilidades técnicas de los sistemas de información.	Analista de Sistemas	Gerente de Tecnología	1/2/2022	16/2/2022
	DG-PAC-26	Documentar y llevar una bitácora de eventos o logs, que ayuden a mitigar las amenazas.	Analista de Sistemas	Gerente de Tecnología	17/2/2022	28/2/2022
	DG-PAC-27	Formación y concienciación a *key users* o *c-levels* acerca de sus responsabilidades referentes a seguridad de la información	Analista de Sistemas	Gerente de Tecnología	1/2/2022	28/2/2022
	DG-PAC-28	Socializar y concientizar al personal, sobre la seguridad de la información.	Analista de Procesos	Gerente de Tecnología	1/3/2022	31/3/2022
	DG-PAC-29	Obtener información técnica oportuna de vulnerabilidades de sistemas de información.	Analista de Infraestructura	Gerente de Tecnología	1/4/2022	15/4/2022
	DG-PAC-30	Implementar una política alineada a un marco de referencia para eliminación y periodo de permanencia e datos.	Analista de Sistemas	Gerente de Tecnología	16/4/2022	24/4/2022

	DG-PAC-31	Adopción de medidas de seguridad fuera de las instalaciones de la organización.	Analista de Infraestructura	Gerente de Tecnología	15/11/2021	15/5/2022
	DG-PAC-32	Asegurar que el suministro de tecnología de información y comunicación, cumpla con los requisitos de tratamiento de seguridad informática.	Analista de Infraestructura	Gerente de Tecnología	1/5/2022	15/5/2022
	DG-PAC-33	Aislar y asegurar las áreas de procesamiento de información, así como la ubicación de sus equipos y servicios.	Analista de Infraestructura	Gerente de Tecnología	15/11/2021	15/5/2022
	DG-PAC-34	Registro de eventos de conexión	Analista de Infraestructura	Gerente de Tecnología	15/11/2021	15/5/2022
	DG-PAC-35	Implementar procedimientos de conexión segura y gestión de contraseñas.	Analista de Infraestructura	Gerente de Tecnología	15/11/2021	15/5/2022
	DG-PAC-36	Implementar un sistema de segundo factor de autenticación	Analista de Infraestructura	Gerente de Tecnología	15/11/2021	15/5/2022
	DG-PAC-37	Implementar una federación de identidades	Analista de Infraestructura	Gerente de Tecnología	15/11/2021	15/5/2022
	DG-PAC-38	Evaluación física periódica de sitios de procesamiento de información.	Analista de Infraestructura	Gerente de Tecnología	15/11/2021	15/5/2022

	DG-PAC-39	Asegurar y evaluar periódicamente los acuerdos con los proveedores, resaltando los riesgos relacionados con la seguridad de la información.	Analista de Sistemas	Gerente de Tecnología	15/11/2021	16/5/2022
	DG-PAC-40	Establecer un estándar de equipamiento y lograr acuerdos de confidencialidad con servicio técnico de proveedores o asociados.	Analista de Sistemas	Gerente de Tecnología	15/11/2021	16/5/2022
	DG-PAC-41	Establecer planes de seguridad de información con buenas prácticas basados en experiencias de terceros para mitigar posibles eventos.	Analista de Sistemas	Gerente de Tecnología	15/11/2021	16/5/2022
	DG-PAC-42	Establecer los limites basados en experiencias o eventos suscitados en organizaciones con giros de negocio similares.	Analista de Infraestructura	Gerente de Tecnología	15/11/2021	16/5/2022
	DG-PAC-43	Implementar un plan de resiliencia y evaluación de hardware.	Analista de Infraestructura	Gerente de Tecnología	1/5/2022	31/5/2022
	DG-PAC-44	Implementar un plan de respuesta a incidentes, el cual debe ser accesible y documentado.	Analista de Sistemas	Gerente de Tecnología	1/5/2022	31/5/2022

	DG-PAC-45	Socializar e implementar prácticas para el uso de información de autenticación secreta	Analista de Procesos	Gerente de Tecnología	17/5/2022	17/6/2022
	DG-PAC-46	Definir un lugar diferente y seguro para almacenamiento de medios.	Analista de Infraestructura	Gerente de Tecnología	18/6/2022	20/6/2022
	DG-PAC-47	Establecer reglas de uso de activos	Analista de Sistemas	Gerente de Tecnología	21/6/2022	28/6/2022
	DG-PAC-48	Establecer un plan de mantenimiento y aseguramiento de la integridad de equipos.	Analista de Infraestructura	Gerente de Tecnología	29/6/2022	15/7/2022
	DG-PAC-49	Establecer un procedimiento y cronograma de mantenimiento de activos por medios remotos.	Analista de Infraestructura	Gerente de Tecnología	29/6/2022	15/7/2022
	DG-PAC-50	Realizar un plan de evaluación de respaldos y medios de almacenamiento de información, así como sus accesos.	Analista de Sistemas	Gerente de Tecnología	16/7/2022	31/7/2022
	DG-PAC-51	Establecer una base de conocimiento referente a incidentes de seguridad informática.	Analista de Sistemas	Gerente de Tecnología	1/8/2022	6/8/2022

	DG-PAC-52	Crear una base de conocimiento de acuerdo con los incidentes y eventos ocurridos.	Analista de Sistemas	Gerente de Tecnología	1/8/2022	6/8/2022
	DG-PAC-53	Realizar una clasificación de la información, basada en la privacidad, valor y confidencialidad.	Analista de Infraestructura	Gerente de Tecnología	12/7/2021	14/8/2022
	DG-PAC-54	Documentar incidentes o posibles intentos de ataques.	Analista de Infraestructura	Gerente de Tecnología	7/8/2022	16/8/2022
	DG-PAC-55	Establecer un procedimiento de recuperación ante incidentes de seguridad informática.	Analista de Sistemas	Gerente de Tecnología	17/8/2022	2/9/2022
	DG-PAC-56	Realizar una revisión de los tipos de información que se entregan.	Analista de Procesos	Gerente de Tecnología	3/9/2022	10/9/2022
	DG-PAC-57	Establecer un plan de gestión de vulnerabilidades.	Analista de Sistemas	Gerente de Tecnología	11/9/2022	30/9/2022
	DG-PAC-58	Implementar políticas y acciones para tratamiento de riesgos	Analista de Sistemas	Gerente de Tecnología	16/4/2022	10/10/2022
	DG-PAC-59	Crear una base de conocimiento de procedimiento, incidentes y eventos.	Analista de Infraestructura	Gerente de Tecnología	1/10/2022	10/10/2022
	DG-PAC-60	Evaluación de espacios físicos	Analista de Infraestructura	Gerente de Tecnología	11/10/2022	21/10/2022

	DG-PAC-61	Implementación de políticas para uso de activos.	Analista de Infraestructura	Gerente de Tecnología	22/10/2022	31/10/2022
	DG-PAC-62	Identificar requisitos legales vigentes, derechos de propiedad intelectual y asegurar la protección de activos de información.	Analista de Procesos	Gerente de Tecnología	15/11/2021	15/11/2022
	DG-PAC-63	Implementación de Políticas y procedimientos para garantizar la seguridad de la información.	Analista de Sistemas	Gerente de Tecnología	15/11/2021	15/11/2022
	DG-PAC-64	Establecer restricciones y gestión de control de cambios.	Analista de Procesos	Gerente de Tecnología	15/11/2021	15/11/2022
	DG-PAC-65	Implementar gestión de cambio	Analista de Procesos	Gerente de Tecnología	15/11/2021	15/11/2022
	DG-PAC-66	Establecer control de cambios de software.	Analista de Sistemas	Gerente de Tecnología	15/11/2021	15/11/2022
	DG-PAC-67	Establecer canales de gestión adecuados para el tratamiento de incidentes.	Analista de Sistemas	Gerente de Tecnología	15/10/2022	15/11/2022
	DG-PAC-68	Establecer acuerdos de colaboración con firmas o proveedores forenses en seguridad de la información.	Analista de Infraestructura	Gerente de Tecnología	10/11/2022	15/11/2022
	DG-PAC-69	Implementar plan de comunicación oportuna.	Analista de Procesos	Gerente de Tecnología	15/11/2022	25/11/2022

	DG-PAC-70	Establecer canales de comunicación oficiales y centralizados.	Analista de Procesos	Gerente de Tecnología	25/11/2022	30/11/2022
	DG-PAC-71	Verificación de continuidad de seguridad de la información ante incidentes o situaciones adversas.	Analista de Infraestructura	Gerente de Tecnología	1/12/2022	8/12/2022
	DG-PAC-72	Establecer controles con grupos de interés.	Analista de Procesos	Gerente de Tecnología	30/11/2022	05/30/2023
	DG-PAC-73	Realizar seguimiento y revisión de servicios contratados con proveedores.	Analista de Sistemas	Gerente de Tecnología	15/11/2021	Continuo
	DG-PAC-74	Llevar a cabo un programa de formación y concientización de seguridad de la información.	Analista de Procesos	Gerente de Tecnología	1/12/2021	Continuo
	DG-PAC-75	Gestionar los cambios de los servicios de proveedores	Analista de Sistemas	Gerente de Tecnología	15/11/2021	Continuo
	DG-PAC-76	Realizar evaluaciones periódicas de funcionamiento de entorno.	Analista de Infraestructura	Gerente de Tecnología	15/11/2021	Continuo
	DG-PAC-77	Establecer una bitácora de actualización de ambiente de pruebas.	Analista de Sistemas	Gerente de Tecnología	15/11/2021	Continuo
	DG-PAC-78	Revisión periódica de eventos de terceros que sirvan como referencia para mitigar posibles incidentes	Analista de Infraestructura	Gerente de Tecnología	15/11/2022	Continuo

	DG-PAC-79	Realizar seguimiento de proveedores de servicios y sistemas de información	Analista de Sistemas	Gerente de Tecnología	15/11/2021	Continuo
	DG-PAC-80	Actualización frecuente de políticas	Analista de Procesos	Gerente de Tecnología	15/11/2021	Continuo
	DG-PAC-81	Revisión de cumplimiento de procesos de tratamiento de información de cada área.	Analista de Procesos	Gerente de Tecnología	15/11/2021	Continuo
	DG-PAC-82	Exigir a todos los involucrados, reporten cualquier debilidad de seguridad de la información observada o sospechada.	Analista de Procesos	Gerente de Tecnología	15/11/2021	Continuo
	DG-PAC-83	Priorizar comunicaciones internas y externas para dar respuesta a incidentes de seguridad informática.	Analista de Procesos	Gerente de Tecnología	1/7/2022	Continuo
	DG-PAC-84	Socializar y supervisar planes de seguridad de la información.	Analista de Sistemas	Gerente de Tecnología	1/6/2022	Continuo
Activos Críticos	AC-PAC-01	Diseñar e Implementar políticas de usuarios y socializarlos con el personal.	Analista de Procesos	Gerente de Tecnología	15/11/2021	30/11/2021
	AC-PAC-02	Delegación adecuada de tareas.	Analista de Sistemas	Gerente de Tecnología	1/12/2021	15/12/2021
	AC-PAC-03	Diseñar e Implementar política de usuarios Administradores.	Analista de Sistemas	Gerente de Tecnología	16/12/2021	22/12/2021

	AC-PAC-04	Diseñar y Establecer políticas de Segregación y delegación de funciones.	Analista de Procesos	Gerente de Tecnología	23/12/2021	31/12/2021
	AC-PAC-05	Diseñar e Implementar políticas de contraseñas y responsabilidad.	Analista de Sistemas	Gerente de Tecnología	3/1/2022	31/1/2022
	AC-PAC-06	Diseñar e Implementar planes de capacitación a personal técnico.	Analista de Sistemas	Gerente de Tecnología	1/2/2022	28/2/2022
	AC-PAC-07	Diseñar e Implementar un plan de control de cambios.	Analista de Procesos	Gerente de Tecnología	1/3/2022	31/3/2022
	AC-PAC-08	Diseñar y aplicar políticas de Respaldos.	Analista de Sistemas	Gerente de Tecnología	1/4/2022	15/4/2022
	AC-PAC-09	Diseñar y Aplicar Políticas de destrucción de información.	Analista de Sistemas	Gerente de Tecnología	16/4/2022	24/4/2022
	AC-PAC-10	Activar y administrar notificaciones y alertas.	Analista de Infraestructura	Gerente de Tecnología	24/4/2022	30/4/2022
	AC-PAC-11	Diseño e Implementación de un plan de contingencia y continuidad de negocio.	Analista de Sistemas	Gerente de Tecnología	1/5/2022	31/5/2022
	AC-PAC-12	Diseñar y Aplicar un plan de renovación y adquisición de soluciones de seguridad para infraestructura.	Analista de Infraestructura	Gerente de Tecnología	1/6/2022	15/6/2022

	AC-PAC-13	Diseñar y Aplicar un plan de mejora y reforzamiento de *software*.	Analista de Sistemas	Gerente de Tecnología	16/6/2022	30/6/2022
	AC-PAC-14	Diseñar e Implementar políticas y procedimientos para accesos de usuarios recursos de ERP.	Analista de Sistemas	Gerente de Tecnología	1/7/2022	15/7/2022
	AC-PAC-15	Establecer perfiles de usuarios bien definidos.	Analista de Sistemas	Gerente de Tecnología	16/7/2022	31/7/2022
	AC-PAC-16	Diseñar e Implementar planes de capacitación periódicos.	Analista de Procesos	Gerente de Tecnología	1/8/2022	12/8/2022
	AC-PAC-17	Diseño e Implementación de políticas claras y formales de uso de sistemas de la información.	Analista de Sistemas	Gerente de Tecnología	13/8/2022	24/8/2022
	AC-PAC-18	Diseñar e Implementar Políticas de uso de recursos empresariales.	Analista de Sistemas	Gerente de Tecnología	25/8/2022	31/8/2022
	AC-PAC-19	Diseñar e Implementar una política de control de cambios.	Analista de Procesos	Gerente de Tecnología	1/9/2022	12/9/2022
	AC-PAC-20	Utilizar eventos extendidos de SQL *Server*.	Analista de Infraestructura	Gerente de Tecnología	13/9/2022	16/9/2022
	AC-PAC-21	Activar Auditoria de SQL *Server*	Analista de Infraestructura	Gerente de Tecnología	17/9/2022	30/9/2022

Adaptado de (ISO (Internacional Organization for Standardization), 2013)

3. CONCLUSIONES

Se evidencia que los procesos son precarios o básicos y en algunos casos inexistentes, o están definidos de manera muy informal, lo cual deja una brecha amplia para poder comprometer la información y sus activos.

La organización es vulnerable a cualquier evento o ataque relacionado con la seguridad de la información que maneja, tanto externo como interno, ya que no cuenta con las herramientas y controles necesarios para mitigar posibles amenazas.

Es prioritario ejecutar los planes de acción a la brevedad posible, dando prioridad a los puntos más críticos, para de esta manera poner a resguardo la información y sus activos críticos.

Este Desarrollo ha tomado las mejores prácticas de varios estándares y permitirá a la organización contar con un proceso de respuesta ante incidentes de seguridad de la información.

Referencias

Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos* (Vol. II). Madrid: © Ministerio de Hacienda y Administraciones Públicas. Obtenido de https://administracionelectronica.gob.es/pae_Home

ISACA. (2018). *Marco de Referencia COBIT® 2019: Objetivos de gobierno y gestión.* Schaumburg. Obtenido de www.isaca.org

ISO (Internacional Organization for Standardization). (2013). *ISO/IEC 27001 Information technology-Security techniques-Information security management systems-Requirements* (Second Edition ed.). Geneva, Switzerland. Obtenido de www.iso.org

ISO (Internacional Organization for Standardization). (2013). *ISO/IEC 27002 Information technology — Security techniques — Code of practice for information security controls* (Second Edition ed.). Geneva, Switzerland. Obtenido de www.iso.org

Juan Carlos López, P. (22 de Abril de 2021). PROYECTO CAPSTONE: Desarrollo del Programa del Sistema de Gestión de Seguridad de la Información de una Organización. Quito, Pichincha, Ecuador. Recuperado el Abril de 2021

National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity* (Vol. 1.1). Gaithersburg. Obtenido de https://doi.org/10.6028/NIST.CSWP.04162018

Salinas, W., Vargas, C. G., & Santana, A. C. (Marzo de 2021). Taller de Apetito al Riesgo, Impacto y evaluación de Tipos de Información. Quito, Pichincha, Ecuador.

ANEXOS

Anexo A

Tabla 1. Análisis de Situación Actual de SGSI Según NIST referenciado con ISO 27001

Función	Categoría	Subcategoría	Referencias informativas	Situación Actual	Ponderación	Detalle
IDENTIFICAR (ID)	**Gestión de activos (ID.AM):** Los datos, el personal, los dispositivos, los sistemas y las instalaciones que permiten a la organización alcanzar los objetivos empresariales se identifican y se administran de forma coherente con su importancia relativa para los	**ID.AM-1:** Los dispositivos y sistemas físicos dentro de la organización están inventariados.	**ISO/IEC 27001:2013** A.8.1.1, A.8.1.2	Medio	10	Inventario de equipos de cómputo y comunicaciones
		ID.AM-2: Las plataformas de software y las aplicaciones dentro de la organización están inventariadas.	**ISO/IEC 27001:2013** A.8.1.1, A.8.1.2	Medio	10	Inventario de software instalado en equipos
		ID.AM-3: La comunicación organizacional y los flujos de datos están mapeados.	**ISO/IEC 27001:2013** A.13.2.1, A.13.2.2	Nulo	0	Inexistente o incipiente
		ID.AM-4: Los sistemas de información externos están catalogados.	**ISO/IEC 27001:2013** A.11.2.6	Nulo	0	Inexistente o incipiente

	objetivos organizativos y la estrategia de riesgos de la organización.	**ID.AM-5:** Los recursos (por ejemplo, hardware, dispositivos, datos, tiempo, personal y software) se priorizan en función de su clasificación, criticidad y valor comercial.	**ISO/IEC 27001:2013** A.8.2.1	Nulo	0	Inexistente o incipiente
		ID.AM-6: Los roles y las responsabilidades de la seguridad cibernética para toda la fuerza de trabajo y terceros interesados (por ejemplo, proveedores, clientes, socios) están establecidas.	**ISO/IEC 27001:2013** A.6.1.1	Bajo	5	Acuerdos con proveedores de servicios y ERP.
	Entorno empresarial (ID.BE): Se entienden y se priorizan la misión, los objetivos, las partes interesadas y las actividades de la organización; esta información	**ID.BE-1:** Se identifica y se comunica la función de la organización en la cadena de suministro.	**ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2	Bajo	5	Existen acuerdos, mas no una gestión de cambios.
		ID.BE-2: Se identifica y se comunica el lugar de la organización en la	**ISO/IEC 27001:2013** Cláusula 4.1	Medio	10	Entendimiento de giro de negocio y su propósito.

	se utiliza para informar los roles, responsabilidades y decisiones de gestión de los riesgos de seguridad cibernética.	infraestructura crítica y su sector industrial.				
		ID.BE-3: Se establecen y se comunican las prioridades para la misión, los objetivos y las actividades de la organización.	**COBIT 5** APO02.01, APO02.06, APO03.01	Medio	10	Misión Visión y Valores
		ID.BE-4: Se establecen las dependencias y funciones fundamentales para la entrega de servicios críticos.	**ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3	Medio	10	Cuenta con sistema de alimentación ininterrumpida y cableado estructurado
		ID.BE-5: Los requisitos de resiliencia para respaldar la entrega de servicios críticos se establecen para todos los estados operativos (p. ej. bajo coacción o ataque, durante la recuperación y operaciones normales).	**ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1	Nulo	0	Inexistente o incipiente
	Gobernanza (ID.GV): Las políticas, los procedimientos y	**ID.GV-1:** Se establece y se comunica la política de seguridad cibernética organizacional.	**ISO/IEC 27001:2013** A.5.1.1	Nulo	0	Inexistente o incipiente

	los procesos para administrar y monitorear los requisitos regulatorios, legales, de riesgo, ambientales y operativos de la organización se comprenden y se informan a la **gestión del riesgo de seguridad cibernética.**	**ID.GV-2:** Los roles y las responsabilidades de seguridad cibernética están coordinados y alineados con roles internos y socios externos.	**ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.15.1.1	Bajo	5	Practicas alineadas a las políticas de seguridad no documentadas.
		ID.GV-3: Se comprenden y se gestionan los requisitos legales y regulatorios con respecto a la seguridad cibernética, incluidas las obligaciones de privacidad y libertades civiles.	**ISO/IEC 27001:2013** A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5	Nulo	0	Inexistente o incipiente
		ID.GV-4: Los procesos de gobernanza y gestión de riesgos abordan los riesgos de seguridad cibernética.	**COBIT 5** EDM03.02, APO12.02, APO12.05, DSS04.02 **ISO/IEC 27001:2013** Cláusula 6	Nulo	0	Inexistente o incipiente
	Evaluación de riesgos (ID.RA): La organización comprende el	**ID.RA-1:** Se identifican y se documentan las vulnerabilidades de los activos.	**ISO/IEC 27001:2013** A.12.6.1, A.18.2.3	Bajo	5	Se determinan vulnerabilidades de activos.

	riesgo de seguridad cibernética para las operaciones de la organización (incluida la misión, las funciones, la imagen o la reputación), los activos de la organización y las personas.	**ID.RA-2:** La inteligencia de amenazas cibernéticas se recibe de foros y fuentes de intercambio de información.	**ISO/IEC 27001:2013** A.6.1.4	Nulo	0	Inexistente o incipiente
		ID.RA-3: Se identifican y se documentan las amenazas, tanto internas como externas.	**ISO/IEC 27001:2013** Cláusula 6.1.2	Bajo	5	Existe una identificación la cual se manifiesta de manera informal y no se encuentra documentada
		ID.RA-4: Se identifican los impactos y las probabilidades del negocio.	**ISO/IEC 27001:2013** A.16.1.6, Cláusula 6.1.2	Nulo	0	Inexistente o incipiente
		ID.RA-5: Se utilizan las amenazas, las vulnerabilidades, las probabilidades y los impactos para determinar el riesgo.	**ISO/IEC 27001:2013** A.12.6.1	Nulo	0	Inexistente o incipiente
		ID.RA-6: Se identifican y priorizan las respuestas al riesgo.	**ISO/IEC 27001:2013** Cláusula 6.1.3	Nulo	0	Inexistente o incipiente
	Estrategia de gestión de riesgos (ID.RM): Se establecen las prioridades,	**ID.RM-1:** Los actores de la organización establecen, gestionan y acuerdan los procesos de gestión de riesgos.	**ISO/IEC 27001:2013** Cláusula 6.1.3, Cláusula 8.3, Cláusula 9.3	Bajo	5	Existen procedimientos informales no documentados.

	restricciones, tolerancias de riesgo y suposiciones de la organización y se usan para respaldar las decisiones de riesgos operacionales.	**ID.RM-2:** La tolerancia al riesgo organizacional se determina y se expresa claramente.	**ISO/IEC 27001:2013** Cláusula 6.1.3, Cláusula 8.3	Bajo	5	Practicas orientadas a mitigar el riesgo, que no se han socializado adecuadamente.
		ID.RM-3: La determinación de la tolerancia del riesgo de la organización se basa en parte en su rol en la infraestructura crítica y el análisis del riesgo específico del sector.	**ISO/IEC 27001:2013** Cláusula 6.1.3, Cláusula 8.3	Bajo	5	Análisis del riesgo básico, sin marcos de referencia
	Gestión del riesgo de la cadena de suministro (ID.SC): Las prioridades, limitaciones, tolerancias de riesgo y suposiciones de la organización se establecen y se utilizan para respaldar las decisiones de riesgo asociadas	**ID.SC-1:** Los actores de la organización identifican, establecen, evalúan, gestionan y acuerdan los procesos de gestión del riesgo de la cadena de suministro cibernética.	**ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2	Nulo	0	Inexistente o incipiente
		ID.SC-2: Los proveedores y socios externos de los sistemas de información, componentes y servicios se identifican, se priorizan y se evalúan mediante un proceso de	**ISO/IEC 27001:2013** A.15.2.1, A.15.2.2	Nulo	0	Inexistente o incipiente

	con la gestión del riesgo de la cadena de suministro. La organización ha establecido e implementado los procesos para identificar, evaluar y gestionar los riesgos de la cadena de suministro.	evaluación de riesgos de la cadena de suministro cibernético.				
		ID.SC-3: Los contratos con proveedores y socios externos se utilizan para implementar medidas apropiadas diseñadas para cumplir con los objetivos del programa de seguridad cibernética de una organización y el plan de gestión de riesgos de la cadena de suministro cibernético.	**ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3	Nulo	0	Inexistente o incipiente
		ID.SC-4: Los proveedores y los socios externos se evalúan de forma rutinaria mediante auditorías, resultados de pruebas u otras formas de evaluación para confirmar que cumplen con sus obligaciones contractuales.	**ISO/IEC 27001:2013** A.15.2.1, A.15.2.2	Nulo	0	Inexistente o incipiente

		ID.SC-5: Las pruebas y la planificación de respuesta y recuperación se llevan a cabo con proveedores.	**ISO/IEC 27001:2013** A.17.1.3	Nulo	0	Inexistente o incipiente
PROTEGER (PR)	**Gestión de identidad, autenticación y control de acceso (PR.AC):** El acceso a los activos físicos y lógicos y a las instalaciones asociadas está limitado a los usuarios, procesos y dispositivos autorizados, y se administra de forma coherente con el riesgo evaluado de acceso no autorizado a actividades	**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.	**ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3	Medio	10	Control de usuarios en ERP y Servicios Cloud
		PR.AC-2: Se gestiona y se protege el acceso físico a los activos.	**ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8	Nulo	0	Inexistente o incipiente

	autorizadas y transacciones.	**PR.AC-3:** Se gestiona el acceso remoto.	**ISO/IEC 27001:2013** A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1	Bajo	5	Habilitación de acceso remoto según el rol o perfil, con el principio del mínimo privilegio.
		PR.AC-4: Se gestionan los permisos y autorizaciones de acceso con incorporación de los principios de menor privilegio y separación de funciones.	**ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5	Medio	10	Manejo de perfiles de usuarios
		PR.AC-5: Se protege la integridad de la red (por ejemplo, segregación de la red, segmentación de la red).	**ISO/IEC 27001:2013** A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3	Nulo	0	Inexistente o incipiente
		PR.AC-6: Las identidades son verificadas y vinculadas a credenciales y afirmadas en las interacciones.	**ISO/IEC 27001:2013**, A.7.1.1, A.9.2.1	Nulo	0	Inexistente o incipiente

		PR.AC-7: Se autentican los usuarios, dispositivos y otros activos (por ejemplo, autenticación de un solo factor o múltiples factores) acorde al riesgo de la transacción (por ejemplo, riesgos de seguridad y privacidad de individuos y otros riesgos para las organizaciones).	**ISO/IEC 27001:2013 A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4**	Bajo	5	Autenticación con contraseñas de un solo factor y gestión de cancelación o revocación de privilegios de cuentas.
	Concienciación y capacitación (PR.AT): El personal y los socios de la organización reciben educación de concienciación sobre la seguridad cibernética y son capacitados para cumplir con sus deberes y responsabilidades relacionados con la seguridad cibernética, en	**PR.AT-1:** Todos los usuarios están informados y capacitados.	**ISO/IEC 27001:2013** A.7.2.2, A.12.2.1	Bajo	5	Capital humano con conocimientos básicos de seguridad de la información.
		PR.AT-2: Los usuarios privilegiados comprenden sus roles y responsabilidades.	**ISO/IEC 27001:2013** A.6.1.1, A.7.2.2	Bajo	5	Usuarios claves con responsabilidades y roles asignados.
		PR.AT-3: Los terceros interesados (por ejemplo, proveedores, clientes, socios) comprenden sus roles y responsabilidades.	**ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.7.2.2	Bajo	5	Acuerdos con proveedores de servicios y ERP.
		PR.AT-4: Los ejecutivos superiores comprenden	**ISO/IEC 27001:2013** A.6.1.1, A.7.2.2	Bajo	5	Empoderamiento de procesos por parte de la supervisión.

	conformidad con las políticas, los procedimientos y los acuerdos relacionados al campo.	sus roles y responsabilidades.				
		PR.AT-5: El personal de seguridad física y cibernética comprende sus roles y responsabilidades.	**ISO/IEC 27001:2013** A.6.1.1, A.7.2.2	Medio	10	Políticas y procedimientos informales, sin documentar
	Seguridad de los datos (PR.DS): La información y los registros (datos) se gestionan en función de la estrategia de riesgo de la organización para proteger la confidencialidad, integridad y disponibilidad de la información.	**PR.DS-1:** Los datos en reposo están protegidos.	**ISO/IEC 27001:2013** A.8.2.3	Alto	20	Los medios físicos están debidamente custodiados y almacenados
		PR.DS-2: Los datos en tránsito están protegidos.	**ISO/IEC 27001:2013** A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3	Medio	10	Encriptación en intercambio de datos de ERP
		PR.DS-3: Los activos se gestionan formalmente durante la eliminación, las transferencias y la disposición.	**ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7	Bajo	5	Solo personal autorizado retira y entrega activos.
		PR.DS-4: Se mantiene una capacidad adecuada para asegurar la disponibilidad.	**ISO/IEC 27001:2013** A.12.1.3, A.17.2.1	Medio	10	Entorno redundante para garantizar la conectividad y el acceso a servicios.

		PR.DS-5: Se implementan protecciones contra las filtraciones de datos.	**ISO/IEC 27001:2013** A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4, **A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3**	Nulo	0	Inexistente o incipiente
		PR.DS-6: Se utilizan mecanismos de comprobación de la integridad para verificar el software, el firmware y la integridad de la información.	**ISO/IEC 27001:2013** A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4	Nulo	0	Inexistente o incipiente

		PR.DS-7: Los entornos de desarrollo y prueba(s) están separados del entorno de producción.	**ISO/IEC 27001:2013** A.12.1.4	Medio	10	Existe dos ambientes, pruebas y producción.
		PR.DS-8: Se utilizan mecanismos de comprobación de la integridad para verificar la integridad del hardware.	**ISO/IEC 27001:2013** A.11.2.4	Bajo	5	Se realiza una revisión esporádica de equipos de computo y comunicaciones.
	Procesos y procedimientos de protección de la información (PR.IP): Se mantienen y se utilizan políticas de seguridad (que abordan el propósito, el alcance, los roles, las responsabilidades, el compromiso de la jefatura y la coordinación entre	**PR.IP-1:** Se crea y se mantiene una configuración de base de los sistemas de control industrial y de tecnología de la información con incorporación de los principios de seguridad (por ejemplo, el concepto de funcionalidad mínima).	**ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4	Bajo	5	Uso responsable de equipos y no instalación de software no autorizado
		PR.IP-2: Se implementa un ciclo de vida de desarrollo del sistema para gestionar los sistemas.	**ISO/IEC 27001:2013** A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5	Nulo	0	Inexistente o incipiente

	las entidades de la organización), procesos y procedimientos para gestionar la protección de los sistemas de información y los activos.	**PR.IP-3:** Se encuentran establecidos procesos de control de cambio de la configuración.	**ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4	Nulo	0	Inexistente o incipiente
		PR.IP-4: Se realizan, se mantienen y se prueban copias de seguridad de la información.	**ISO/IEC 27001:2013** A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3	Nulo	0	Inexistente o incipiente
		PR.IP-5: Se cumplen las regulaciones y la política con respecto al entorno operativo físico para los activos organizativos.	**ISO/IEC 27001:2013** A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3	Nulo	0	Inexistente o incipiente
		PR.IP-6: Los datos son eliminados de acuerdo con las políticas.	**ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7	Bajo	5	No existe política formal de eliminación de datos.
		PR.IP-7: Se mejoran los procesos de protección.	**ISO/IEC 27001:2013** A.16.1.6, Cláusula 9,	Nulo	0	Inexistente o incipiente

			Cláusula 10			
		PR.IP-8: Se comparte la efectividad de las tecnologías de protección.	**ISO/IEC 27001:2013** A.16.1.6	Nulo	0	Inexistente o incipiente
		PR.IP-9: Se encuentran establecidos y se gestionan planes de respuesta (Respuesta a Incidentes y Continuidad del Negocio) y planes de recuperación (Recuperación de Incidentes y Recuperación de Desastres).	**ISO/IEC 27001:2013** A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3	Bajo	5	Procedimientos de restablecimiento de comunicaciones y equipos, no formalizado.
		PR.IP-10: Se prueban los planes de respuesta y recuperación.	**ISO/IEC 27001:2013** A.17.1.3	Nulo	0	Inexistente o incipiente
		PR.IP-11: La seguridad cibernética se encuentra incluida en las prácticas de recursos humanos (por ejemplo, desaprovisionamiento, selección del personal).	**ISO/IEC 27001:2013** A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4	Bajo	5	Proceso de salida de personal en el cual se registra y los equipos a cargo y se da de baja las cuentas corporativas.

		PR.IP-12: Se desarrolla y se implementa un plan de gestión de las vulnerabilidades.	**ISO/IEC 27001:2013** A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.2, A.18.2.3	Nulo	0	Inexistente o incipiente
	Mantenimiento (PR.MA): El mantenimiento y la reparación de los componentes del sistema de información y del control industrial se realizan de acuerdo con las políticas y los procedimientos.	**PR.MA-1:** El mantenimiento y la reparación de los activos de la organización se realizan y están registrados con herramientas aprobadas y controladas.	**ISO/IEC 27001:2013** A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6	Medio	10	Las tareas de mantenimiento y reparación de equipos, se realiza únicamente por personal autorizado.
		PR.MA-2: El mantenimiento remoto de los activos de la organización se aprueba, se registra y se realiza de manera que evite el acceso no autorizado.	**ISO/IEC 27001:2013** A.11.2.4, A.15.1.1, A.15.2.1	Nulo	0	Inexistente o incipiente
	Tecnología de protección (PR.PT): Las soluciones técnicas de	**PR.PT-1:** Los registros de auditoría o archivos se determinan, se documentan, se implementan y se revisan	**ISO/IEC 27001:2013** A.12.4.1, A.12.4.2, A.12.4.3,	Bajo	5	El ERP maneja auditoria

	seguridad se gestionan para garantizar la seguridad y la capacidad de recuperación de los sistemas y activos, en consonancia con las políticas, procedimientos y acuerdos relacionados.	en conformidad con la política.	A.12.4.4, A.12.7.1			
		PR.PT-2: Los medios extraíbles están protegidos y su uso se encuentra restringido de acuerdo con la política.	**ISO/IEC 27001:2013** A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9	Nulo	0	Inexistente o incipiente
		PR.PT-3: Se incorpora el principio de menor funcionalidad mediante la configuración de los sistemas para proporcionar solo las capacidades esenciales.	**ISO/IEC 27001:2013** A.9.1.2	Bajo	5	Configuración y operación de servicios requeridos.
		PR.PT-4: Las redes de comunicaciones y control están protegidas.	**ISO/IEC 27001:2013** A.13.1.1, A.13.2.1, A.14.1.3	Bajo	5	Firewall básico sin control de navegación o accesos
		PR.PT-5: Se implementan mecanismos (por ejemplo, a prueba de fallas, equilibrio de carga, cambio en caliente o “hot swap”) para lograr los	**ISO/IEC 27001:2013** A.17.1.2, A.17.2.1	Nulo	0	Inexistente o incipiente

		requisitos de resiliencia en situaciones normales y adversas.				
DETECTAR (DE)	**Anomalías y Eventos (DE.AE):** se detecta actividad anómala y se comprende el impacto potencial de los eventos.	**DE.AE-1:** Se establece y se gestiona una base de referencia para operaciones de red y flujos de datos esperados para **los usuarios y sistemas.**	**ISO/IEC 27001:2013** A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2	Bajo	5	Base de referencia y procedimientos no definidos formalmente
		DE.AE-2: Se analizan los eventos detectados para comprender los objetivos y métodos de ataque.	**ISO/IEC 27001:2013** A.12.4.1, A.16.1.1, A.16.1.4	Nulo	0	No ha existido incidentes
		DE.AE-3: Los datos de los eventos se recopilan y se correlacionan de múltiples fuentes y sensores.	**ISO/IEC 27001:2013** A.12.4.1, A.16.1.7	Nulo	0	No ha existido incidentes
		DE.AE-4: Se determina el impacto de los eventos.	**ISO/IEC 27001:2013** A.16.1.4	Nulo	0	No ha existido incidentes
		DE.AE-5: Se establecen umbrales de alerta de incidentes.	**ISO/IEC 27001:2013** A.16.1.4	Nulo	0	Inexistente o incipiente

	Monitoreo Continuo de la Seguridad (DE.CM): El sistema de información y los activos son monitoreados a fin de identificar eventos de seguridad cibernética y verificar la eficacia de las medidas de protección.	**DE.CM-1:** Se monitorea la red para detectar posibles eventos de seguridad cibernética.	**COBIT 5** DSS01.03, DSS03.05, DSS05.07	Bajo	5	Revisión de equipos conectados a la red.
		DE.CM-2: Se monitorea el entorno físico para detectar posibles eventos de seguridad cibernética.	**ISO/IEC 27001:2013** A.11.1.1, A.11.1.2	Nulo	0	Inexistente o incipiente
		DE.CM-3: Se monitorea la actividad del personal para detectar posibles eventos de seguridad cibernética.	**ISO/IEC 27001:2013** A.12.4.1, A.12.4.3	Nulo	0	Inexistente o incipiente
		DE.CM-4: Se detecta el código malicioso.	**ISO/IEC 27001:2013** A.12.2.1	Bajo	5	Software antivirus-endpoint instalado en equipos.
		DE.CM-5: Se detecta el código móvil no autorizado.	**ISO/IEC 27001:2013** A.12.5.1, A.12.6.2	Nulo	0	Inexistente o incipiente
		DE.CM-6: Se monitorea la actividad de los proveedores de servicios externos para detectar posibles eventos de seguridad cibernética.	**ISO/IEC 27001:2013** A.14.2.7, A.15.2.1	Nulo	0	Inexistente o incipiente

		DE.CM-7: Se realiza el monitoreo del personal, conexiones, dispositivos y software no autorizados.	**ISO/IEC 27001:2013** A.12.4.1, A.14.2.7, A.15.2.1	Bajo	5	Revisión periódica de equipos y dispositivos conectados a la red.
		DE.CM-8: Se realizan escaneos de vulnerabilidades.	**ISO/IEC 27001:2013 A.12.6.1**	Nulo	0	Inexistente o incipiente
	Procesos de Detección (DE.DP): Se mantienen y se aprueban los procesos y procedimientos de detección para garantizar el conocimiento de los eventos anómalos.	**DE.DP-1:** Los roles y los deberes de detección están bien definidos para asegurar la responsabilidad.	**ISO/IEC 27001:2013** A.6.1.1, A.7.2.2	Nulo	0	Inexistente o incipiente
		DE.DP-2: Las actividades de detección cumplen con todos los requisitos aplicables.	**ISO/IEC 27001:2013** A.18.1.4, A.18.2.2, A.18.2.3	Nulo	0	Inexistente o incipiente
		DE.DP-3: Se prueban los procesos de detección.	**ISO/IEC 27001:2013** A.14.2.8	Nulo	0	Inexistente o incipiente
		DE.DP-4: Se comunica la información de la detección de eventos.	**ISO/IEC 27001:2013** A.16.1.2, A.16.1.3	Bajo	5	Se reporta a la gerencia de sistemas, los eventos detectados de seguridad de la información.
		DE.DP-5: los procesos de detección se mejoran continuamente.	**ISO/IEC 27001:2013** A.16.1.6	Bajo	5	Existe un reporte al gerente de sistemas mas no un proceso formal.

RESPONDER (RS)	**Planificación de la Respuesta (RS.RP):** Los procesos y procedimientos de respuesta se ejecutan y se mantienen a fin de garantizar la respuesta a los incidentes de seguridad cibernética detectados.	**RS.RP-1:** El plan de respuesta se ejecuta durante o después de un incidente.	**ISO/IEC 27001:2013** A.16.1.5	Nulo	0	No ha existido incidentes
	Comunicaciones (RS.CO): Las actividades de respuesta se coordinan con las partes interesadas internas y externas (por ejemplo, el apoyo externo de organismos encargados de hacer cumplir la ley).	**RS.CO-1:** El personal conoce sus roles y el orden de las operaciones cuando se necesita una respuesta.	**ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, A.16.1.1	Bajo	5	Procesos informales, no existe claridad en responsabilidades
		RS.CO-2: Los incidentes se informan de acuerdo con los criterios establecidos.	**ISO/IEC 27001:2013** A.6.1.3, A.16.1.2	Bajo	5	Se reporta a la gerencia de sistemas, pero no existe departamento formal de seguridad de la información
		RS.CO-3: La información se comparte de acuerdo con los planes de respuesta.	**ISO/IEC 27001:2013** A.16.1.2, Cláusula 7.4,	Nulo	0	Inexistente o incipiente

			Cláusula 16.1.2			
		RS.CO-4: La coordinación con las partes interesadas se realiza en consonancia con los planes de respuesta.	**ISO/IEC 27001:2013** Cláusula 7.4	Nulo	0	Inexistente o incipiente
		RS.CO-5: El intercambio voluntario de información se produce con las partes interesadas externas para lograr una mayor conciencia situacional de seguridad cibernética.	**ISO/IEC 27001:2013** A.6.1.4	Nulo	0	Inexistente o incipiente
	Análisis (RS.AN): Se lleva a cabo el análisis para garantizar una respuesta eficaz y apoyar las actividades de recuperación.	**RS.AN-1:** Se investigan las notificaciones de los sistemas de detección.	**ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.5	Nulo	0	No ha existido incidentes
		RS.AN-2: Se comprende el impacto del incidente.	**ISO/IEC 27001:2013** A.16.1.4, A.16.1.6	Nulo	0	Inexistente o incipiente
		RS.AN-3: Se realizan análisis forenses.	**ISO/IEC 27001:2013** A.16.1.7	Nulo	0	Inexistente o incipiente

		RS.AN-4: Los incidentes se clasifican de acuerdo con los planes de respuesta.	**ISO/IEC 27001:2013** A.16.1.4	Nulo	0	Inexistente o incipiente
		RS.AN-5: Se establecen procesos para recibir, analizar y responder a las vulnerabilidades divulgadas a la organización desde fuentes internas y externas (por ejemplo, pruebas internas, boletines de seguridad o investigadores de seguridad).	**COBIT 5** EDM03.02, DSS05.07	Nulo	0	Inexistente o incipiente
	Mitigación (RS.MI): Se realizan actividades para evitar la expansión de un evento, mitigar sus efectos y resolver el incidente.	**RS.MI-1:** Los incidentes son contenidos.	**ISO/IEC 27001:2013** A.12.2.1, A.16.1.5	Nulo	0	Inexistente o incipiente
		RS.MI-2: Los incidentes son mitigados.	**ISO/IEC 27001:2013** A.12.2.1, A.16.1.5	Nulo	0	Inexistente o incipiente
		RS.MI-3: Las vulnerabilidades recientemente identificadas son	**ISO/IEC 27001:2013** A.12.6.1	Bajo	5	Revisión de logs de endpoints

		mitigadas o se documentan como riesgos aceptados.				
	Mejoras (RS.IM): Las actividades de respuesta de la organización se mejoran al incorporar las lecciones aprendidas de las actividades de detección y respuesta actuales y previas.	**RS.IM-1:** Los planes de respuesta incorporan las lecciones aprendidas.	**ISO/IEC 27001:2013** A.16.1.6, Cláusula 10	Nulo	0	Inexistente o incipiente
		RS.IM-2: Se actualizan las estrategias de respuesta.	**ISO/IEC 27001:2013** A.16.1.6, Cláusula 10	Nulo	0	Inexistente o incipiente
RECUPERAR (RC)	**Planificación de la recuperación (RC.RP):** Los procesos y procedimientos de recuperación se ejecutan y se mantienen para asegurar la restauración de los sistemas o activos afectados por incidentes de	**RC.RP-1:** El plan de recuperación se ejecuta durante o después de un incidente de seguridad cibernética.	**ISO/IEC 27001:2013** A.16.1.5	Nulo	0	Inexistente o incipiente

	seguridad cibernética.					
	Mejoras (RC.IM): La planificación y los procesos de recuperación se mejoran al incorporar en las actividades futuras las lecciones aprendidas.	**RC.IM-1:** Los planes de recuperación incorporan las lecciones aprendidas.	**ISO/IEC 27001:2013** A.16.1.6, Cláusula 10	Nulo	0	No ha existido incidentes
		RC.IM-2: Se actualizan las estrategias de recuperación.	**ISO/IEC 27001:2013** A.16.1.6, Cláusula 10	Nulo	0	No ha existido incidentes
	Comunicaciones (RC.CO): Las actividades de restauración se coordinan con partes internas y externas (por ejemplo, centros de coordinación, proveedores de servicios de	**RC.CO-1:** Se gestionan las relaciones públicas.	**ISO/IEC 27001:2013** A.6.1.4, Cláusula 7.4	Nulo	0	No ha existido incidentes
		RC.CO-2: La reputación se repara después de un incidente.	**ISO/IEC 27001:2013** Cláusula 7.4	Nulo	0	No ha existido incidentes
		RC.CO-3: Las actividades de recuperación se comunican a las partes	**ISO/IEC 27001:2013** Cláusula 7.4	Nulo	0	No ha existido incidentes

	Internet, propietarios de sistemas de ataque, víctimas, otros CSIRT y vendedores).	interesadas internas y externas, así como también a los equipos ejecutivos y de administración.			

Adaptado de (National Institute of Standards and Technology, 2018)

Anexo B

Tabla 2 Métricas Según Actividad de COBIT5 utilizadas con NIST.

BAI09.01	a. Porcentaje de activos registrados correctamente en el registro de activos
	b. Porcentaje de activos que son adecuados para su propósito
	c. Porcentaje de activos en inventario y actualizados
BAI09.02	a. Número de activos críticos
	b. Promedio de inactividad por activo crítico
	c. Número de tendencias de incidentes identificadas
BAI09.05	a. Porcentaje de licencias utilizadas frente a licencias adquiridas
	b. Porcentaje de licencias que se siguen pagando pero que no se usan
	c. Porcentaje de productos y licencias que deberían actualizarse para lograr un mayor valor
DSS05.02	a. Número de brechas del firewall
	b. Número de vulnerabilidades descubiertas
	c. Porcentaje de tiempo que la red y los sistemas no están disponibles debido a incidentes de seguridad
APO02.02	a. Porcentaje de personal satisfecho con sus capacidades actuales
	b. Porcentaje de satisfacción del Dueño de negocio con la inversión y la utilización de la base de activos interna y externa para cumplir con factores críticos de éxito
APO10.04	a. Frecuencia de las sesiones de gestión de riesgos con el proveedor
	b. Número de eventos relacionados con riesgos que conducen a incidentes de servicio
	c. Porcentaje de incidentes relacionados con el riesgo resueltos de manera aceptable (en tiempo y coste)
DSS01.02	a. Número de KPI específicos/SMART incluidos en los contratos de externalización
	b. Frecuencia de falla del socio subcontratista para cumplir con los KPI
APO03.03	a. Número de brechas identificadas en los modelos empresariales de los dominios de arquitectura del negocio, la información, los datos, la aplicación y la tecnología.

	b. Porcentaje de partes interesadas clave del negocio y de TI para evaluar la disposición de transformación de la empresa e identificar oportunidades, soluciones y todas las restricciones de implementación.
APO03.04	a. Definición clara de los requisitos de gobierno para la implementación de la arquitectura.
	b. Porcentaje de partes interesadas conocedoras de la implementación y migración de la arquitectura.
APO12.01	a. Número de eventos de pérdida con características clave capturados en repositorios
	b. Porcentaje de auditorías, eventos y tendencias capturados en repositorios
	c. Porcentaje de sistemas críticos con problemas conocidos
BAI04.02	a. Número de escenarios creados para evaluar situaciones de disponibilidad futuras
	b. Porcentaje de dueños de procesos de negocio que aprueban los resultados del análisis
APO01.02	a. Frecuencia de comunicación de los objetivos y dirección de gestión para I&T
	b. Asignación de responsabilidad para el envío de comunicaciones regulares
APO07.06	a. Porcentaje de contratistas que firman el marco de control empresarial
	b. Frecuencia de las revisiones periódicas llevadas a cabo para garantizar la exactitud y el cumplimiento con la ley, del personal del contratista.
APO13.01	a. Nivel de satisfacción de las partes interesadas con el plan de seguridad en toda la empresa
DSS06.03	a. Número de incidentes y hallazgos de auditoría debido a violaciones de acceso o de separación de funciones
	b. Porcentaje de roles de procesos de negocio con derechos de acceso y niveles de autoridad asignados
	c. Porcentaje de roles de proceso de negocio con clara separación de funciones
APO08.01	a. Número de problemas empresariales actuales identificados
	b. Números de requisitos empresariales definidos para servicios habilitados por I&T

APO08.04	a. Tiempo transcurrido desde la última actualización del plan de comunicación para toda la empresa
	b. Porcentaje de satisfacción del dueño de negocio con la coordinación de la prestación íntegra de servicios y soluciones de I&T
APO08.05	a. Porcentaje de servicios de I&T alineados con los requisitos de negocio de la empresa
	b. Porcentaje de las causas raíz identificadas y resueltas para todos los problemas
APO10.03	a. Porcentaje de terceros proveedores que tienen contratos que definen los requisitos de control
	b. Número de disputas formales con proveedores
	c. Número de reuniones de revisión con los proveedores
	d. Porcentaje de disputas resueltas amistosamente en un plazo razonable
APO10.05	a. Número de incumplimientos en los servicios relacionados con I&T causados por los proveedores
	b. Porcentaje de proveedores que cumplen con los requisitos acordados
APO02.06	a. Frecuencia de actualizaciones del plan de comunicación de la estrategia de I&T
	b. Porcentaje de partes interesadas conocedoras de la dirección y estrategia de I&T
APO03.01	a. Nivel de retroalimentación de los clientes sobre la arquitectura
	b. Grado en el que las arquitecturas base y objetivo cubren los dominios del negocio, la información, los datos, la aplicación y la tecnología.
APO02.01	a. Nivel de conocimiento dentro de la dirección de I&T de la organización y contextos empresariales actuales
	b. Nivel de conocimiento dentro de la dirección de I&T de las metas y dirección empresariales
	c. Nivel de conocimiento de las partes interesadas claves sobre I&T y sus requisitos específicos
APO10.01	a. Porcentaje de criterios de evaluación definidos logrados para los proveedores externos y contratos vigentes
	b. Porcentaje de proveedores externos alternativos que proporcionan servicios equivalentes a contratos de proveedores externos vigentes

BAI03.02	a. Número de deficiencias en la revisión del diseño
	b. Número de cambios de diseño en proceso
DSS04.02	a. Inactividad total derivada de un incidente o interrupción importante.
	b. Porcentaje de partes interesadas claves involucradas en el análisis de impacto del negocio que evalúan el impacto a lo largo del tiempo de duración de una interrupción de funciones críticas del negocio y el efecto que una interrupción tendría sobre ellas
APO01.03	a. Número de procesos prioritarios que deben implementarse o mejorarse para cumplir con el nivel de capacidad objetivo
	b. Número de métricas definidas para el seguimiento de la implementación satisfactoria del proceso
EDM01.01	a. Número de principios guía definidos para el gobierno y la toma de decisiones de I&T
	b. Número de altos ejecutivos implicados en establecer el rumbo del gobierno para I&T
EDM01.02	a. Grado en el cual los principios de gobierno de I&T acordados son evidentes en procesos y prácticas (porcentaje de procesos y prácticas que se atribuyen a los principios)
	b. Frecuencia de presentación de informes del gobierno de I&T al comité ejecutivo y el consejo de administración
	c. Número de roles, responsabilidades y autoridades para el gobierno de I&T que son definidos, asignados y aceptados por los directivos de negocio e I&T correspondientes.
APO13.02	a. Porcentaje de simulaciones de escenarios de riesgo de seguridad exitosas
	b. Número de empleados que han completado con éxito una formación de concienciación sobre seguridad de la información
DSS05.04	a. Tiempo promedio entre el cambio y la actualización de cuentas
	b. Número de cuentas (vs. número de usuarios/personal autorizado)
	c. Número de incidentes relacionados con el acceso no autorizado a la información
BAI02.01	a. Porcentaje de requisitos reelaborados debido a la falta de alineación con las necesidades y expectativas de la empresa

	b. Porcentaje de los requisitos validados a través de enfoques como revisión realizada por colegas, validación del modelo o construcción de prototipos operativos
MEA03.01	a. Frecuencia de revisiones de requisitos de cumplimiento
	b. Porcentaje de satisfacción de las partes interesadas clave en el proceso de revisión del cumplimiento normativo.
MEA03.04	a. Número de informes de cumplimiento obtenidos
	b. Porcentaje de cumplimiento de los proveedores de servicio basado en revisiones independientes
	c. Tiempo transcurrido entre la identificación de la brecha de cumplimiento y la acción correctora
	d. Número de informes de acciones correctivas que tratan brechas de cumplimiento cerradas oportunamente
EDM03.02	a. Nivel de alineamiento entre el riesgo de I&T y el riesgo empresarial
	b. Porcentaje de proyectos de la empresa que consideran el riesgo de I&T.
APO12.02	a. Número de escenarios de riesgo de I&T identificados
	b. Tiempo transcurrido desde la última actualización de los escenarios de riesgos de I&T
APO12.05	a. Número de incidentes significativos no identificados e incluidos en el portafolio de gestión de riesgos
	b. Porcentaje de propuestas de proyectos de gestión de riesgos rechazadas por falta de consideración de otros riesgos relacionados
APO12.03	a. Completitud de atributos y valores en el perfil de riesgo
	b. Porcentaje de procesos clave de negocio incluidos en el perfil de riesgo
APO12.04	a. Nivel de satisfacción de las partes interesadas con los informes de riesgos proporcionados
	b. Completitud de los informes del perfil de riesgos (incluida información alineada con los requisitos de las partes interesadas)
	c. Uso de informes de riesgos en la toma de decisiones de gestión
DSS05.01	a. Número de ataques exitosos de software malicioso
	b. Porcentaje de empleados que no pasan las pruebas de ataques maliciosos (p.ej., la prueba de correos electrónicos de phishing)

BAI08.01	a. Porcentaje de información clasificada validada
	b. Porcentaje de pertinencia de los tipos de contenido, artefactos e información estructurada y no estructurada
BAI02.03	a. Porcentaje de riesgos de los requisitos no cubiertos por una adecuada respuesta al riesgo
	b. Nivel de detalle del riesgo de los requisitos documentado
	c. Qué tan completa es la probabilidad estimada y el impacto del riesgo de los requisitos y las respuestas al riesgo enumerados
APO12.06	a. Número de medidas que no reducen el riesgo residual
	b. Porcentaje de planes de acción de riesgo de I&T ejecutados según se diseñaron
BAI01.03	a. Nivel de satisfacción de las partes interesadas con su compromiso
	b. Porcentaje de partes interesadas involucradas de manera efectiva
APO10.02	a. Número de brechas identificadas entre las ofertas del proveedor seleccionado y las necesidades señaladas en la solicitud de propuesta (RFP)
	b. Porcentaje de partes interesadas satisfechas con los proveedores
MEA01.01	a. Porcentaje de procesos con metas y métricas definidos
	b. Porcentaje de integración del enfoque de supervisión en el sistema de gestión de rendimiento corporativo
MEA01.02	a. Porcentaje de metas y métricas aprobadas por las partes interesadas
	b. Porcentaje de procesos con revisión y mejora de la efectividad de metas y métricas
MEA01.03	a. Porcentaje de procesos críticos supervisados
	b. Porcentaje del entorno de controles que es supervisado, analizado comparativamente y mejorado para cumplir con los objetivos de la organización
MEA01.04	a. Porcentaje de metas y métricas alineadas con el sistema de supervisión de la empresa
	b. Porcentaje de informes de desempeño enviados conforme al plazo
	c. Porcentaje de procesos con resultado asegurado en línea con los objetivos y dentro de las tolerancias
MEA01.05	a. Número de anomalías recurrentes
	b. Número de acciones correctivas implementadas

DSS04.04	a. Frecuencia de las pruebas
	b. Número de ejercicios y pruebas que alcanzaron los objetivos de recuperación
DSS01.04	a. Número de personas capacitadas para responder a los procedimientos de alarma medioambiental
	b. Número de escenarios de riesgo definidos para las amenazas medioambientales
DSS05.05	a. Calificación promedio de las evaluaciones de seguridad física
	b. Número de incidentes relacionados con la seguridad de la información física
DSS05.03	a. Número de incidentes que involucran a dispositivos *endpoint*.
	b. Número de dispositivos no autorizados detectados en la red o en el entorno de usuario final
	c. Porcentaje de personas que reciben formación de concienciación relacionada con el uso de dispositivos *endpoint*.
DSS01.05	a. Tiempo transcurrido desde la última prueba del suministro de energía ininterrumpida
	b. Número de personas formadas en normas de salud y seguridad
DSS05.07	a. Número de pruebas de vulnerabilidad llevadas a cabo en dispositivos perimetrales
	b. Número de vulnerabilidades descubiertas durante las pruebas
	c. Tiempo dedicado a remediar vulnerabilidades
	d. Porcentaje de tiques creados de forma oportuna cuando los sistemas de monitorización identifican posibles incidentes de seguridad.
APO07.03	a. Identificar habilidades y competencias clave que no se encuentren en la matriz de recursos
	b. Número de brechas identificadas entre las habilidades requeridas y las disponibles
	c. Número de programas de capacitación proporcionados
BAI05.07	a. Número de capacitaciones y transferencias de conocimientos realizadas
	b. Porcentaje de participación de la alta dirección en el refuerzo del cambio

APO07.02	a. Porcentaje de trabajos críticos en los que la empresa depende de un único individuo
	b. Número de planes de respaldo de personal realizados
APO01.06	a. Número de partes interesadas claves que han aprobado el establecimiento de la función de TI
	b. Porcentaje de partes interesadas con una opinión favorable del establecimiento de la función de TI
BAI06.01	a. Cantidad de retrabajo causado por cambios fallidos
	b. Porcentaje de cambios sin éxito debidos a evaluaciones de impacto inadecuadas
DSS04.07	a. Porcentaje de medios de respaldo transferidos y almacenados de forma segura
	b. Porcentaje de restauración exitosa y oportuna de copias de seguridad o copias de medios alternativos
DSS06.06	a. Casos de datos de transacciones sensibles enviados al destinatario erróneo
	b. Frecuencia de integridad de datos críticos comprometida
BAI09.03	a. Porcentaje de activos gestionados desde la adquisición hasta su disposición
	b. Porcentaje de uso por activo
	c. Porcentaje de activos desplegados que siguen el ciclo de vida de implementación estándar
BAI04.04	a. Número de eventos que exceden los límites de capacidad planificados
	b. Número de picos de transacciones que exceden el rendimiento objetivo
DSS06.02	a. Número de incidentes y hallazgos de auditoría que indican un fallo de los controles clave
	b. Porcentaje de cobertura de controles clave dentro de los planes de prueba
BAI03.08	a. Número de errores encontrados durante la prueba
	b. Tiempo y esfuerzo para completar las pruebas
BAI07.04	a. Nivel de comparación entre el entorno de pruebas y el entorno operativo y de negocio futuro
	b. Nivel de datos (y/o bases de datos) de pruebas borrados de forma segura (sanitizados) que son representativos del entorno de producción
BAI03.05	a. Brecha entre el esfuerzo de desarrollo estimado frente al esfuerzo de desarrollo final

	b. Número de problemas de software comunicados
	c. Número de errores revisados
BAI10.01	a. Número de partes interesadas que aprueban el modelo de configuración
	b. Porcentaje de precisión de las relaciones entre los elementos de configuración
BAI10.02	a. Número de elementos de configuración (CI) listados en el repositorio
	b. Porcentaje de precisión sobre las líneas de referencia de la configuración de un servicio, aplicación o infraestructura
BAI10.03	a. Frecuencia de cambios/actualizaciones al repositorio
	b. Porcentaje de precisión e integridad del repositorio de Cis
BAI10.05	a. Número de desviaciones entre el repositorio de configuración y la configuración real
	b. Número de discrepancias en relación con la información de configuración incompleta o faltante
BAI03.01	a. Número de deficiencias de la revisión del diseño
	b. Porcentaje de participación de las partes interesadas en el diseño y la aprobación de cada versión.
BAI03.03	a. Número de excepciones al diseño de la solución observadas durante la etapa de revisión.
	b. Número de diseños detallados para los procesos del negocio, servicios de soporte, aplicaciones e infraestructura y repositorios de información
BAI01.06	a. Porcentaje de beneficios de programas esperados y logrados
	b. Porcentaje de programas para los cuales se monitorizo el rendimiento y la acción remedial oportuna se llevó a cabo cuando fue necesario
DSS01.01	a. Número de incidentes causados por problemas operativos
	b. Número de procedimientos operativos no estándar ejecutados
DSS05.06	a. Número de dispositivos de salida robados.
	b. Porcentaje de documentos sensibles y dispositivos de salida identificados en el inventario
DSS04.05	a. Porcentaje de mejoras acordadas para el plan que se han incorporado al plan
	b. Porcentaje de planes de continuidad y evaluaciones del impacto en el negocio que se encuentran actualizados

BAI08.04	a. Frecuencia de actualización
	b. Nivel de satisfacción de los usuarios
DSS03.04	a. Reducir el número de incidentes recurrentes causados por problemas no resueltos
	b. Porcentaje de soluciones temporales definidas para los problemas abiertos
DSS04.03	a. Número de sistemas críticos de negocio no cubiertos por el plan
	b. Porcentaje de partes interesadas claves involucradas en el desarrollo de BCPs y DRPs
APO07.01	a. Duración promedio de las vacantes
	b. Porcentaje de puestos de TI vacantes
	c. Porcentaje de rotación de personal
APO07.04	a. Número de momentos de retroalimentación oficial y evaluaciones de 360 grados realizadas
	b. Número y valor de las recompensas otorgadas al personal
APO07.05	a. Número de carencias identificadas y habilidades ausentes a la hora de planificar el personal
	b. Tiempo utilizado por cada empleado a tiempo completo en trabajos y proyectos
BAI03.10	a. Número de demandas de mantenimiento no satisfechas
	b. Duración de las demandas de mantenimiento que se satisfacen y no se satisfacen
APO11.04	a. Porcentaje de soluciones y servicios entregados con certificación formal
	b. Calificación promedio de satisfacción de las partes interesadas con las soluciones y los servicios
	c. Número de procesos con un reporte formal de evaluación de la calidad
	d. Porcentaje de proyectos revisados que cumplen con las metas y los objetivos de calidad esperados
	e. Número, robustez y plazo de los análisis de riesgo
MEA02.01	a. Número de brechas mayores de control interno
	b. Porcentaje de entorno de controles y marco supervisados, analizados comparativamente y mejorados continuamente para cumplir con los objetivos de la organización
BAI04.01	a. Porcentaje de uso real de la capacidad
	b. Porcentaje de disponibilidad real
	c. Porcentaje de rendimiento real

BAI04.03	a. Número de actualizaciones no planificadas de capacidad, rendimiento o disponibilidad
	b. Porcentaje comparaciones realizadas por la dirección sobre la demanda actual de recursos contra la oferta y demanda estimadas
BAI04.05	a. Número y porcentaje de incidencias de disponibilidad, rendimiento y capacidad sin resolver
	b. Número de incidentes de disponibilidad
DSS03.01	a. Porcentaje de incidentes mayores para los que se registraron problemas
	b. Porcentaje de incidentes resueltos conforme a los SLA acordados
	c. Porcentaje de problemas identificados correctamente, incluida la clasificación, categorización y priorización de estos.
BAI08.02	a. Número de relaciones identificadas entre las fuentes de información (etiquetado)
	b. Porcentaje de satisfacción de las partes interesadas con la organización y contextualización de la información en conocimiento
DSS01.03	a. Porcentaje de tipos de eventos operativos críticos cubiertos por sistemas de detección automática
	b. Porcentaje de activos de infraestructura monitorizados conforme a la criticidad del servicio y la relación entre los elementos de configuración y servicios que dependen de ellos
DSS03.05	a. Porcentaje de problemas registrados como parte de la actividad de gestión de problemas proactiva
	b. Porcentaje de partes interesadas satisfechas con la comunicación de información de problemas relacionados con cambios e incidentes de TI
DSS06.01	a. Porcentaje de inventario de procesos críticos y controles clave completado
	b. Porcentaje de controles de procesamiento alineados con las necesidades empresariales
MEA03.03	a. Número de problemas críticos de incumplimiento identificados cada año
	b. Porcentaje de dueños de procesos que aprueban y confirman el cumplimiento
DSS02.05	a. Porcentaje de incidentes resueltos dentro de los SLA acordados

	b. Porcentaje de satisfacción de las partes interesadas con la solución y recuperación del incidente
DSS02.04	a. Número de síntomas de incidentes identificados y registrados
	b. Número de causas de síntomas correctamente determinadas
	c. Número de problemas duplicados en el log de referencia
DSS02.07	a. Tiempo promedio entre incidentes para el servicio habilitado por I&T
	b. Número y porcentaje de incidentes que causan interrupciones en procesos críticos del negocio
DSS02.02	a. Número de tipos y categorías definidos para registrar solicitudes e incidentes de servicio
	b. Número de solicitudes e incidentes de servicio no clasificados
DSS03.02	a. Número de problemas identificados clasificados como errores conocidos
	b. Porcentaje de problemas investigados y diagnosticados a lo largo de su ciclo de vida
DSS04.08	a. Porcentaje de problemas identificados que se han abordado posteriormente en el plan
	b. Porcentaje de problemas identificados que se han abordado posteriormente en los materiales de formación
BAI07.08	a. Número y porcentaje de análisis causa raíz completados
	b. Número o porcentaje de liberaciones que no se estabilizan dentro de un período aceptable
	c. Porcentaje de liberaciones que causan tiempo de inactividad
MEA03.02	a. Tiempo promedio entre la identificación de los problemas de cumplimiento externo y su resolución
	b. Porcentaje de satisfacción del personal relevante con la comunicación de los requisitos de cumplimiento regulatorio, nuevos y modificados

Tomado de (ISACA, 2018)

Nota: En la tabla se muestra en la columna izquierda el código de la actividad o practica y en la derecha está la métrica que corresponde a la actividad.

Anexo C

Tabla 3. Modulador de Apetito y Mapas de Calor

Importación de Vehículos	**Valoración del Impacto**									
	Modulador del apetito			**Niveles de impacto**					**Probabilidad Inherente**	
Descripción del Impacto	**AVERSION**	**NEUTRAL**	**AGRESIVO**	**INSIGNIFICANTE**	**MENOR**	**MODERADO**	**MAYOR**	**CATASTRÓFICO**		
Incumplimiento de entregas	X					< 5días	Entre 5días a 10 días	mayor a 10 días	Probable	4
Gastos mayores a los previstos		X			Gasto hasta 5% sobre el valor del vehículo	Gasto hasta 10% sobre el valor del vehículo	Gasto hasta 15% sobre el valor del vehículo	Gasto mayor al 15% sobre el valor del vehículo	Posible	3
Inventario estancado	X				< 10días	10-15 días	>15 días y <30 días	>30 días	Poco probable	2
Afectación o degradación en la reputación	X						Perdida de 20% de dealers	Perdida de 50% de dealers	Posible	3

Pérdidas económicas por daño de vehículos		X		Sin daños	daños leves que no pasen más del 1% del valor del vehículo	Deterioro de vehículos que represente el 10% del valor	Deterioro de vehículos que represente el 15% del valor	Daño total del vehículo	Raro	1

Tomado de (Salinas, Vargas, & Santana, 2021)

Tabla 4 Mapa de Severidad 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
	CERTEZA	Moderado	Moderado	Alto	Crítico	Crítico

Tomado de (Salinas, Vargas, & Santana, 2021)

Tabla 5 Probabilidad de Ocurrencia

Probabilidad de Ocurrencia	
Raro	1
Poco probable	2
Posible	3
Probable	4
Certeza	5

Tomado de (Salinas, Vargas, & Santana, 2021)

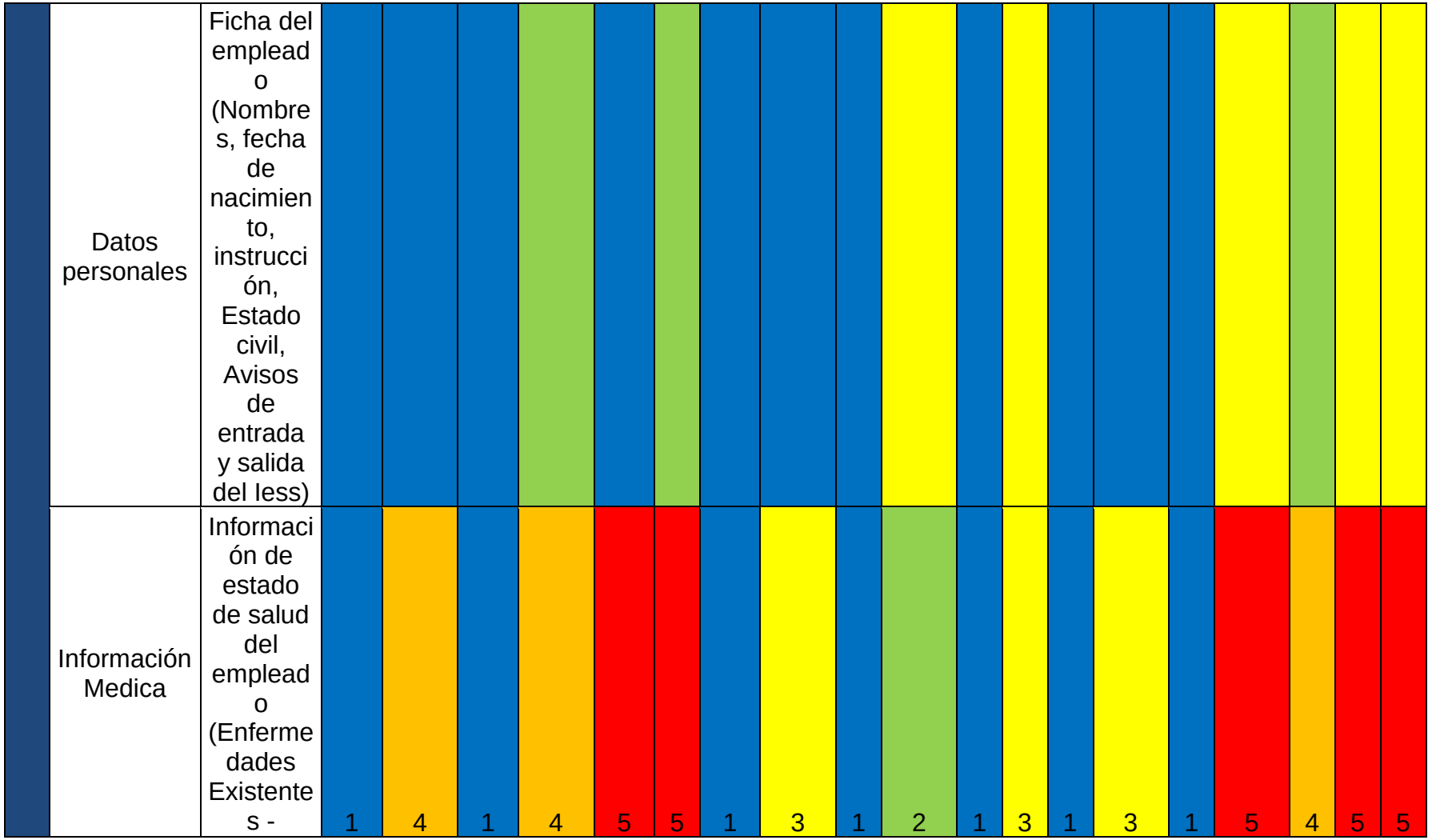
Tabla 6. Evaluación del Tipo de Información

Entidad	Nombre del tipo de información	Tipo de Información	Integridad						Disponibilidad						Confidencialidad						Valoración Máxima de resultados
			Incumplimiento de entregas	Gastos mayores a los previstos	Inventario estancado	Afectación o degradación en la reputación	Pérdidas de ingresos	Resultado	Incumplimiento de entregas	Gastos mayores a los previstos	Inventario estancado	Afectación o degradación en la reputación	Pérdidas de ingresos	Resultado	Incumplimiento de entregas	Gastos mayores a los previstos	Inventario estancado	Afectación o degradación en la reputación	Pérdidas de ingresos	Resultado	
Proveedores	Modelos de Vehículos	Listado de Modelos y versiones de Vehículos	1	1	4	1	4	4	4	1	4	1	2	4	1	1	2	1	1	2	4

	Inventario de Vehículos	Cantidad, Costo y Precio de Vehículos	5	3	5	1	4	5	5	4	5	3	5	5	4	4	5	3	5	5	5
	Información Aduanera	Información Impuestos y aranceles aduaneros	4	4	4	3	5	5	4	4	4	2	4	4	3	3	3	4	4	4	5
	Información Legal	Contratos y Acuerdos de Importación Información Relacionada con Agente Aduanero	4	4	3	4	5	5	4	4	3	3	4	4	3	3	3	4	4	4	5

	Información Bancaria	Detalle de datos para transferencias bancarias al Exterior (Swift, IBAN, etc)	4	4	3	3	4	4	3	4	3	2	2	4	3	3	2	2	2	3	4
Empleados	Domicilio	Datos de dirección de domicilio y referencias	1	1	1	2	1	2	1	1	1	1	1	1	1	1	1	3	2	3	3
	Información Tributaria	Formulario 107, Impuesto a la Renta, RDEP (Anexo de relación de	1	1	1	3	1	3	1	1	1	1	1	1	1	1	1	3	1	3	3

		dependencia)																			
	Información Legal	Juicios de Alimentos Estatus Migratorio Antecedentes Penales Contratos Laborales	1	3	1	3	5	5	1	3	1	3	3	3	1	3	1	3	3	3	5
	Información Bancaria	Datos de cuentas bancarias para pago de nómina, utilidades y otros Beneficios de ley	1	1	1	4	2	4	1	1	1	1	1	1	1	2	1	2	1	2	4
			1	1	1	2	1	2	1	1	1	3	1	3	1	1	1	3	2	3	3


Datos personales
Ficha del empleado (Nombres, fecha de nacimiento, instrucción, Estado civil, Avisos de entrada y salida del Iess)
Información Medica
Información de estado de salud del empleado (Enfermedades Existentes -
1 4 1 4 5 5 1 3 1 2 1 3 1 3 1 5 4 5 5

		Preexistentes, Exámenes Preocupacionales y Ocupacionales, Discapacidades o Sustitutos)																					
	Laborales	Currículo Laboral del empleado (Salario, Cargo, Jefe inmediato, Referencias Laborales,	1	1	1	3	3	3	1	1	1	2	1	2	1	1	1	4	4	4	4

		Historial Laboral)																				
Clientes	Datos de Facturación	Datos de contactabilidad (Identificación, dirección, teléfonos, correo electrónico, contactos)	4	2	1	2	4	4	4	3	2	3	2	4	2	2	2	2	2	2	4
	Información Tributaria	Información relacionada para emisión de retenciones (Tipo de Contribuyente)	1	3	1	3	4	4	2	3	2	2	3	3	2	2	2	3	2	3	4

	Información Unidad de Análisis Financiero (UAFE)	Formularios UAFE Conozca su Cliente	4	3	2	5	3	5	2	2	2	4	3	4	2	1	2	3	2	3	5
	Información Bancaria	Datos bancarios para devoluciones y rebates	2	2	2	4	4	4	1	2	3	3	2	3	2	2	2	2	2	2	4
	Información Dealer	Datos de entrega Contactos y direcciones de Entrega	5	3	3	5	4	5	4	4	4	4	4	4	4	3	2	4	3	4	5
	Información de Marketing	Información de Campañas Publicitarias y Presentaciones	1	3	4	5	5	5	1	4	3	4	4	4	2	4	3	4	5	5	5

		de la Marca																				
	Información de Exonerados	Datos sensibles de Clientes con Capacidades Especiales (Solicitudes, Certificados)	4	3	5	5	5	5	1	4	4	5	5	5	4	3	3	5	5	5	5

Adaptado de (Salinas, Vargas, & Santana, 2021)

Tabla 7. Tabla de Activos Críticos

Entidad	Tipo de Información	Descripción	Activo de Información	Código de Activo	Información Estructurada	Procesos que utilizan el activo	Propietario del Activo	Criticidad
Proveedores	Listado de Modelos y versiones de Vehículos	Carpeta Compartida Logística	Unidad NAS(SYNOLOGY)	ACT-NAS-01	No	Compras y Logística / Comercial	Jefe de Compras / Jefe de Logística	
	Cantidad, Costo y Precio de Vehículos	Módulo de Inventario ERP	Base de Datos ERP (SQL SERVER 2017)	ACT-BDD-01	Si	Compras/Logística	Jefe de Compras / Jefe de Logística / Gerente Comercial	
	Información Impuestos y aranceles aduaneros	Módulo de Compras ERP	Base de Datos ERP (SQL SERVER 2017)	ACT-BDD-01	Si	Financiero / Contable/Logística	Jefe de Logística	
	Contratos y Acuerdos de Importación Información Relacionada con Agente Aduanero	Carpeta Compartida Legal Carpeta Compartida Exportador	Unidad NAS(SYNOLOGY)	ACT-NAS-01	No	Legal /Logística	Contralor / Jefe de Logística	

		Carpeta Contraloría						
	Detalle de datos para transferencias bancarias al Exterior (Swift, IBAN, etc)	Módulo de Registro de Cuentas-BDD ERP Modulo de caja y egresos-BDD ERP	Base de Datos ERP (SQL SERVER 2017)	ACT-BDD-01	Si	Financiero/ Contable	Gerencia Financiera/Contador General	
Empleados	Datos de dirección de domicilio y referencias	Base de datos sistema de nomina	BDD Sistema de gestión de nómina (SQL SERVER 2014)	ACT-BDD-02	Si	Talento Humano	Gerente de RRHH	
	Formulario 107, Impuesto a la Renta, RDEP (Anexo de relación de dependencia)	Base de datos sistema de nomina	BDD Sistema de gestión de nómina (SQL SERVER 2014)	ACT-BDD-02	Si	Talento Humano	Gerente de RRHH	
	Juicios de Alimentos Estatus Migratorio Antecedentes Penales	Base de datos sistema de nomina	BDD Sistema de gestión de nómina (SQL SERVER 2014)	ACT-BDD-02	Si	Talento Humano / Legal	Gerente de RRHH	

	Contratos Laborales							
	Datos de cuentas bancarias para pago de nómina, utilidades y otros Beneficios de ley	Base de datos sistema de nomina	BDD Sistema de gestión de nómina (SQL SERVER 2014)	ACT-BDD-02	Si	Talento Humano / Contable	Gerente de RRHH	
	Ficha del empleado (Nombres, fecha de nacimiento, instrucción, Estado civil, Avisos de entrada y salida del Iess)	Base de datos sistema de nomina	BDD Sistema de gestión de nómina (SQL SERVER 2014)	ACT-BDD-02	Si	Talento Humano / Legal / Contable	Gerente de RRHH	
	Información de estado de salud del empleado (Enfermedades Existentes - Preexistentes, Exámenes Preocupacionales y Ocupacionales, Discapacidades o Sustitutos)	Base de datos sistema de nomina	BDD Sistema de gestión de nómina (SQL SERVER 2014)	ACT-BDD-02	Si	sso / talento humano	Medico Ocupacional	
		Archivo Físico	Anaqueles Físicos de Archivo	ACT-AF-01	No			

	Currículo Laboral del empleado (Salario, Cargo, jefe inmediato, Referencias Laborales, Historial Laboral)	Base de datos sistema de nomina	BDD Sistema de gestión de nómina (SQL SERVER 2014)	ACT-BDD-02	Si	Talento Humano	Gerente de RRHH	
		Archivo Físico	Anaqueles Físicos de Archivo	ACT-AF-01	No			
Clientes	Datos de contactabilidad (Identificación, dirección, teléfonos, correo electrónico, contactos)	ERP Módulos de Terceros	Base de Datos ERP (SQL SERVER 2017)	ACT-BDD-01	Si	Contabilidad Comercial	Gerencia Comercial / Contador General	
	Información relacionada para emisión de retenciones (Tipo de Contribuyente)	ERP Módulos de Terceros	Base de Datos ERP (SQL SERVER 2017)	ACT-BDD-01	Si	Contabilidad	Contador General	
	Formularios UAFE Conozca su Cliente	Carpeta Compartida Carpeta UAFE	Unidad NAS(SYNOLOGY)	ACT-NAS-01	No	UAFE	Oficial de Cumplimiento	
	Datos bancarios para devoluciones y rebates	ERP Modulo de consignación y egresos	Base de Datos ERP (SQL SERVER 2017)	ACT-BDD-01	Si	Contabilidad	Gerente Financiero / Contador General	
					Si	Logística	Jefe de Logística	

	Datos de entrega Contactos y direcciones de Entrega	ERP Modulo de Remisiones	Base de Datos ERP (SQL SERVER 2017)	ACT-BDD-01				
	Información de Campañas Publicitarias y Presentaciones de la Marca	Carpetas Campañas y Presentaciones	Nube Privada (ONEDRIVE)	ACT-NP-01	No	Marketing	Gerencia de Marketing	
	Datos sensibles de Clientes con Capacidades Especiales (Solicitudes, Certificados)	Clientes Exonerados	Nube Privada (ONEDRIVE)	ACT-NP-01	No	Comercial Compras y Logística	Jefe de Logística / Jefe de Compras / Gerencia Comercial	

Anexo D

Tabla 8. Análisis de Amenazas y Vulnerabilidades.

Activo de Información	Tipo de activo	Categoría	Amenazas	Dimensiones	Vulnerabilidades	Identificación en el Activo	Riesgo Inherente			Controles Actuales
							Probabilidad	Impacto	Riesgo	
Base de Datos ERP (SQL SERVER 2017) ACT-BDD-01	[D] Datos Información	[E] Errores y fallos no intencionados	[E.1] Errores de los usuarios	I C D	Acceso a ingresar Información Incorrecta o mal digitada	x	Posible	Mayor	**Alto**	Permisos de ingreso de datos por campos
			[E.2] Errores del administrador	D I C	Ausencia de Proceso de Respaldos Falta de procesos de control de cambios	x	Posible	Catastrófico	**Crítico**	Respaldo automático de BDD

			[E.15] Alteración accidental de la información	I	Falta de formación y capacitación de uso de herramientas al personal.	x	Posible	Mayor	**Alto**	Proceso de capacitación informal
			[E.18] Destrucción de información	D	Ausencia de formación de seguridad de la información del personal. Falta de Políticas de Destrucción de Información.	x	Posible	Catastrófico	**Critico**	No existe
			[E.19] Fugas de información	C	Usuarios con Privilegios Inadecuados Usuarios con accesos a cuentas personales en quipos corporativos Ausencia de políticas de	x	Posible	Mayor	**Alto**	Creación de Roles por Usuario

					confidencialidad					
		[A] Ataques intencionados	[A.5] Suplantación de la identidad del usuario	C A I	Ausencia de Proceso de Gestión de Usuarios Falta de Políticas de usuarios	x	Posible	Catastrófico	**Critico**	Solicitud de alta y baja de usuarios vía correo electrónico
			[A.6] Abuso de privilegios de acceso	C I D	Usuarios con acceso total Usuarios sin segregación de funciones	x	Posible	Mayor	**Alto**	Tablas de auditoria

			[A.11] Acceso no autorizado	C I	Uso de contraseñas por Defecto. Uso de métodos de autenticación inadecuados	x	Posible	Catastrófico	**Critico**	No existe
			[A.15] Modificación deliberada de la información	I	Personal sin Ética Ausencia de logs	x	Poco Probable	Catastrófico	**Alto**	Tablas de auditoria
			[A.18] Destrucción de información	D	Ausencia de planes de contingencia Usuarios con niveles de accesos privilegiados innecesarios.	x	Posible	Catastrófico	**Critico**	No existe

			[A.19] Divulgación de información	C	Ausencia de Herramientas de Seguridad Especializada Uso de canales de comunicación sin cifrar.	x	Posible	Catastrófico	**Critico**	No existe

Adaptado de (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)

Tabla 9. Planes de Acción para mitigar Amenazas y Vulnerabilidades del Activo crítico

Amenazas	Vulnerabilidades	Riesgo Residual	Planes de Acción
[E.1] Errores de los usuarios	Acceso a ingresar Información Incorrecta o mal digitada	**Alto**	**Diseñar e Implementar políticas y procedimientos para accesos de usuarios recursos de ERP.**
			Establecer perfiles de usuarios bien definidos.
[E.2] Errores del administrador	Ausencia de Proceso de Respaldos Falta de procesos de control de cambios	**Alto**	**Diseñar y aplicar políticas de Respaldos.**
			Diseñar e Implementar un plan de control de cambios.
			Delegación adecuada de tareas.
[E.15] Alteración accidental de la información	Falta de formación y capacitación de uso de herramientas al personal.	**Alto**	**Diseñar e Implementar planes de capacitación periódicos.**
[E.18] Destrucción de información	Ausencia de formación de seguridad de la	**Critico**	**Diseñar e Implementar planes de capacitación a personal técnico.**

	información del personal. Falta de Políticas de Destrucción de Información.		**Diseñar y Aplicar Políticas de destrucción de información.**
[E.19] Fugas de información	Usuarios con Privilegios Inadecuados Usuarios con accesos a cuentas personales en quipos corporativos Ausencia de políticas de confidencialidad	**Alto**	**Diseño e Implementación de políticas claras y formales de uso de sistemas de la información.**
			Diseñar e Implementar Políticas de uso de recursos empresariales.
[A.5] Suplantación de la identidad del usuario	Ausencia de Proceso de Gestión de Usuarios Falta de políticas de usuarios	**Alto**	**Diseñar e Implementar políticas de usuarios y socializarlos con el personal.**
[A.6] Abuso de privilegios de acceso	Usuarios con acceso total	**Medio**	**Diseñar e Implementar política de usuarios Administradores.**

	Usuarios sin segregación de funciones		**Diseñar y Establecer políticas de Segregación y delegación de funciones.**
[A.11] Acceso no autorizado	Uso de contraseñas por Defecto. Uso de métodos de autenticación inadecuados	**Critico**	**Diseñar e Implementar políticas de contraseñas y responsabilidad.**
			Activar y administrar notificaciones y alertas.
[A.15] Modificación deliberada de la información	Personal sin ética Ausencia de logs	**Alto**	**Diseñar e Implementar una política de control de cambios.**
			Utilizar eventos extendidos de SQL Server.
			Activar Auditoria de SQL Server
[A.18] Destrucción de información	Ausencia de planes de contingencia Usuarios con niveles de accesos privilegiados innecesarios.	**Critico**	**Diseño e Implementación de un plan de contingencia y continuidad de negocio.**

[A.19] Divulgación de información	Ausencia de Herramientas de Seguridad Especializada Uso de canales de comunicación sin cifrar.	**Critico**	**Diseñar y Aplicar un plan de renovación y adquisición de soluciones de seguridad para infraestructura.**
			Diseñar y Aplicar un plan de mejora y reforzamiento de software.

Adaptado de (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)

RoadMap de Planes de Acción para Mitigar Amenazas y Vulnerabilidades