FORTALECIMIENTO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) EN UNA ENTIDAD EDUCATIVA

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

---

Autoras

María Fernanda Portilla Pedraza

Iliana Rebeca Vargas Pico

Año 2021

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

“Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.”

María Fernanda Portilla Pedraza

1719670463

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

“Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.”

Iliana Rebeca Vargas Pico

1712344611

AGRADECIMIENTOS

“Quiero expresar mi gratitud a Dios,
quien con su bendición llena
siempre mi vida y a toda mi familia
por estar siempre presentes.
Mi profundo agradecimiento
a todas las autoridades y personal
de la UDLA, por confiar en mí,
abrirme las puertas y
permitirme realizar todo el
proceso académico dentro del
establecimiento educativo.”

María Fernanda Portilla Pedraza

AGRADECIMIENTOS

“Gracias a Dios por la vida, la salud,
y por las bendiciones que nos
entrega día a día,
gracias a mi familia que ha sido
mi soporte y mi inspiración para
seguirme superando.
Finalmente, gracias a la UDLA y mis
profesores por los conocimientos
impartidos que serán de ayuda en
mi carrera profesional.”

Iliana Rebeca Vargas Pico

DEDICATORIA

“Dedico esta tesis a mis padres
y hermana quienes fueron
un gran apoyo emocional durante el
tiempo en que escribía esta tesis.
A mi compañera de tesis
quien me apoyo y alentó
para continuar, cuando parecía
que me iba a rendir.”

María Fernanda Portilla Pedraza

DEDICATORIA

“Dedico este trabajo a mi esposo y a
mis hijas por su apoyo, amor y
paciencia para alcanzar este
objetivo. A mis padres y compañera
de trabajo por la fuerza y empuje
para no decaer y concluir
lo que empecé.”

Iliana Rebeca Vargas Pico

RESUMEN

El trabajo de titulación consiste, en el diseño de una propuesta para la ejecución de un programa del Sistema de Gestión de Seguridad de la Información, para una entidad educativa. Mediante el diagnóstico de su situación actual basado en el marco de referencia NIST y Cobit (Information Security), clasificación de la información, inventario de activos críticos, y el análisis de amenazas y vulnerabilidades tomando como referencia los marcos ISO27001.2013 y Magerit v.3 2012.

Como resultado del proceso, se entregará a la entidad educativa el programa inicial para la ejecución del Sistema de Gestión de Seguridad de la Información, así como, las políticas de alto nivel que se deben desarrollar para dar continuidad a este programa.

ABSTRACT

Degree work consists in designing a proposal for the implementation of a program of the Management System Information Security, for an educational institution. By diagnosing your current situation based on the NIST and Cobit (Information Security) reference framework, information classification, inventory of critical assets, and the analysis of threats and vulnerabilities taking as reference the ISO27001.2013 and Magerit v. 3 2012.

As a result of the process, the initial program for the implementation of the Information Security Management System will be delivered to the educational entity, as well as the high-level policies that must be developed to give continuity to this program.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1. INTRODUCCIÓN

El sector de la educación (instituciones educativas de alto nivel) son blanco de ataques cibernéticos, debido al volumen y sensibilidad de datos e información que se administra en sus sistemas.

La información, es de alto valor para los ciberdelincuentes ya que las instituciones educativas gestionan desde: i) datos personales sobre la comunidad estudiantil, ii) datos del personal docente, iii) datos del personal administrativo, iv) información financiera y de investigación.

El entorno de la pandemia por Covid 19, obligó también a las instituciones educativas a implementar mecanismos de teletrabajo y estudio remoto, lo cual implicó un cambio y adaptación no controlada y enfocada en temas de seguridad y gestión de usuarios en los diferentes sistemas y aplicativos de la institución.

El número de amenazas y vulnerabilidades crece constantemente, por lo que es primordial proteger los activos más importantes de la organización, garantizando siempre la disponibilidad, confidencialidad e integridad de la información.

Los ataques cibernéticos más comunes son: *phishing*, hurto de credenciales y ataques e incidentes en el sistema eléctrico.

“Datos informativos: la Asociación Nacional de Universidades e Instituciones de Educación Superior (ANUIES-México)”, indica:

- 56% no cuentan con una política de ciberseguridad.
- 74% no ha efectuado una evaluación certificada de su sistema tecnológico.
- 58% no cuenta con un equipo capacitado y dedicado para temas de Seguridad de la Información. (Expansión México, 2020)

“Según el estudio de Ciberseguridad en Ecuador 2020, solo el 37% de las empresas evaluadas cuentan con un Sistema de Gestión de Seguridad de Información formalizado” (IT Ahora, 2020).

2. DESARROLLO DEL PROYECTO DE TITULACIÓN

2.1. Metodología

En el proyecto se utilizará un método de investigación inductivo, constituido por la formulación de un problema, el planteamiento de una hipótesis, el análisis de los elementos del proyecto, para el diseño de un programa de seguridad de la información basado en NIST, ISO 27001 y COBIT para una entidad educativa.

2.2. Presupuesto

Para la ejecución del proyecto se utilizará los siguientes recursos y presupuesto:

Tabla 1

Presupuesto y Recursos.

Detalle	Cantidad	Precio	Tiempo
Recursos- Personas	2	$ 3.200,00	10 meses de trabajo
Equipos de computación	2	$ 1.000,00	
Herramientas ofimáticas (Word, PPT, Excel)	2	$ 68,00	
Marcos de Referencia (COBIT)	2	$ 0,00	
Total		$ 4.268,00	

2.3. Fases

Las fases aplicadas para el desarrollo del proyecto son:

2.3.1. Diagnóstico

La metodología utilizada en el proyecto para la evaluación de la situación actual del SGSI, en la institución educativa sobre la cual estamos realizando el trabajo, se basa en los siguientes marcos de referencia para Seguridad y Cyber seguridad de la información, los cuales son referentes como mejores prácticas en el mercado.

Los marcos utilizados son NIST y COBIT, a continuación, una breve descripción de cada uno de ellos:

NIST

Es un Framework, con enfoque basado en riesgos, para la gestión de ciberseguridad. Ver figura 1.

Figura 1. Funciones del marco de referencia NIST.
Tomado de (GlobalSUITE, 2018)

"Identificar: Ayuda a desarrollar un entendimiento organizacional para administrar el riesgo de ciberseguridad de los sistemas, las personas, los activos, los datos y las capacidades."

"Proteger: Describe las medidas de seguridad adecuadas para garantizar la entrega de servicios de las infraestructuras críticas."

"Detectar: Define las actividades necesarias para identificar la ocurrencia de un evento de ciberseguridad, permitiendo el descubrimiento oportuno de los mismos."

"Responder: Incluye actividades necesarias para tomar medidas con respecto a un incidente de ciberseguridad detectado, desarrollando la capacidad de contener el impacto de un potencial incidente."

***"Recuperar*:** Identifica las actividades necesarias para mantener los planes de resiliencia y para restaurar cualquier capacidad o servicio que se haya deteriorado debido a un incidente de ciberseguridad." (GlobalSUITE, 2018)

COBIT - INFORMATION SECURITY

"Establece un enfoque holístico de la seguridad y protección de la empresa, definiendo las responsabilidades y elementos que permitan el gobierno y la gestión de la seguridad. Alinea la seguridad de la información con todos los objetivos de la empresa, mediante las prácticas de gobierno y la gestión enfocada a la seguridad." (COBIT Focus Area: Information Security, 2020) Ver figura 2.

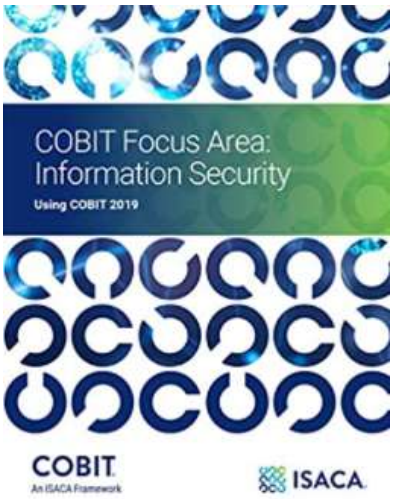


Figura 2. Portada del libro Cobit (Information security).
Tomado de (COBIT Focus Area: Information Security, 2020)

Criterios para evaluación:

En base al framework de mejora en cyber seguridad (NIST) y mediante reuniones con el CISO de la entidad educativa; se procedió a evaluar por cada subcategoría del marco el porcentaje de cumplimiento respecto de seguridad de la información que se mantiene.

El marco de referencia cuenta con cinco funciones, cada una de ellas tiene una categoría y sus respectivas subcategorías de evaluación.

La valoración fue efectuada de la siguiente forma:

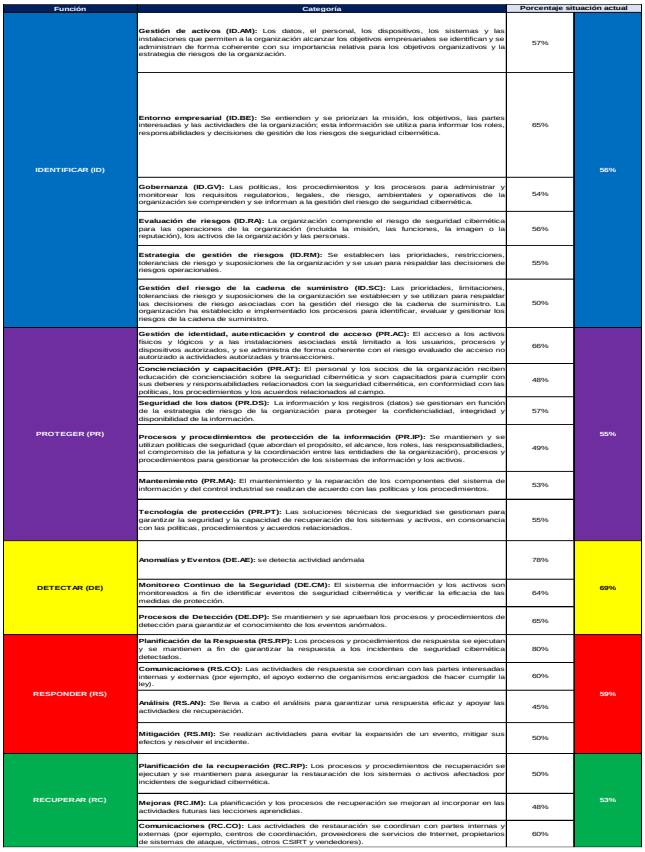
1. Autoevaluación de las actividades que constan en cada subcategoría.

2. Obtención del promedio por cada subcategoría.
   El análisis total se encuentra desarrollado en el Anexo 1. Ver figura 3.

Figura 3. Captura de pantalla del análisis realizado por cada actividad específica.

3. Obtención del promedio por cada categoría.

   El resumen realizado por cada categoría se encuentra desarrollado en el Anexo 1, que corresponde a “Metodología del estado actual SGSI” en la hoja “Resumen por Categoría”. Ver figura 4.



Función	Categoría	Porcentaje situación actual	
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 objetivos organizativos y la estrategia de riesgos de la organización.	57%	56%
	Entorno empresarial (ID.BE): Se entienden y se priorizan la misión, los objetivos, las partes interesadas y las actividades de la organización; esta información se utiliza para informar los roles, responsabilidades y decisiones de gestión de los riesgos de seguridad cibernética.	65%	
	Gobernanza (ID.GV): Las políticas, los procedimientos y 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.	54%	
	Evaluación de riesgos (ID.RA): La organización comprende el 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.	56%	
	Estrategia de gestión de riesgos (ID.RM): Se establecen las prioridades, restricciones, tolerancias de riesgo y suposiciones de la organización y se usan para respaldar las decisiones de riesgos operacionales.	55%	
	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 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.	50%	
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 autorizadas y transacciones.	66%	55%
	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 conformidad con las políticas, los procedimientos y los acuerdos relacionados al campo.	48%	
	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.	57%	
	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 las entidades de la organización), procesos y procedimientos para gestionar la protección de los sistemas de información y los activos.	49%	
	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.	53%	
	Tecnología de protección (PR.PT): Las soluciones técnicas de 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.	55%	
DETECTAR (DE)	**Anomalías y Eventos (DE.AE):** se detecta actividad anómala	78%	69%
	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.	64%	
	Procesos de Detección (DE.DP): Se mantienen y se aprueban los procesos y procedimientos de detección para garantizar el conocimiento de los eventos anómalos.	65%	
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.	80%	59%
	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).	60%	
	Análisis (RS.AN): Se lleva a cabo el análisis para garantizar una respuesta eficaz y apoyar las actividades de recuperación.	45%	
	Mitigación (RS.MI): Se realizan actividades para evitar la expansión de un evento, mitigar sus efectos y resolver el incidente.	50%	
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 seguridad cibernética.	50%	53%
	Mejoras (RC.IM): La planificación y los procesos de recuperación se mejoran al incorporar en las actividades futuras las lecciones aprendidas.	48%	
	Comunicaciones (RC.CO): Las actividades de restauración se coordinan con partes internas y externas (por ejemplo, centros de coordinación, proveedores de servicios de Internet, propietarios de sistemas de ataque, víctimas, otros CSIRT y vendedores).	60%	

Figura 4. Captura de pantalla del análisis realizado por cada categoría.

Finalmente se realiza un promedio por cada categoría para realizar un resumen ejecutivo e identificar el estado actual general, y las oportunidades de mejora, el cual se encuentra desarrollado en el Anexo 1, que corresponde a “Metodología del estado actual SGSI” en la hoja “Informe situación actual”. Ver figura 5.

Función	Porcentaje situación actual	Estado actual por categoría	Oportunidad de mejora	Código.
IDENTIFICAR (ID)	56%	La institución educativa cuenta con un inventario de su infraestructura (servidores, aplicaciones, sistemas y servicios)sin embargo; no se cuenta con una clasificación que identifique los activos de información críticos para la entidad.	Establecer proceso de evaluación de los riesgos de seguridad de la información para identificar los riesgos asociados a la pérdida de la confidencialidad, integridad y disponibilidad de la información. Realizar el levantamiento y clasificación de los activos de información críticos según el tipo de información.	DI-ID-01 DI-ID-02
		La institución educativa mantiene canales apropiados de comunicación entre todas las partes interesadas, para una comunicación efectiva entre seguridad de la información y el negocio. El área de Seguridad de la Información participa activamente en los comités de la organización como parte fundamental para identificar necesidades de implementación de seguridad de la información de forma transversal en todos los servicios. La institución educativa cuenta con non-disclosure agreement en los contratos con los proveedores, personal bajo dependencia laboral; adicionalmente se realizan revisiones del cumplimiento de servicios con terceros.	Definir métricas que permitan medir el cumplimiento de la normativa interna respecto de seguridad de la información. Definir, coordinar, aprobar objetivos y requisitos de seguridad de la información dentro de la arquitectura de la institución. Documentar los controles de seguridad de la información que mantiene la institución e implementar escenarios y actividades de resiliencia para respuesta de ataques internos. Analizar, evaluar y formalizar normativa para ciberseguridad en la institución.	DI-ID-03 DI-ID-04 DI-ID-05 DI-ID-06
		La institución educativa no tiene formalizada la normativa para ciberseguridad, sin embargo se cuentan con herramientas de seguridad que permiten controlar ataques externos.	Analizar, evaluar y formalizar normativa para el gobierno de ciberseguridad en la institución educativa.	DI-ID-07
		La institución educativa no tiene formalizada la normativa para la gestión de riesgos de ciberseguridad, sin embargo se cuentan con herramientas de seguridad que permiten controlar ataques externos.	Analizar, evaluar y formalizar normativa para la evaluación de riesgos de ciberseguridad en la institución educativa.	DI-ID-08
		La institución educativa cuenta con análisis e identificación de vulnerabilidades para los servidores que soportan los aplicativos core, no se ha realizado para el resto de infraestructura (bases de datos, aplicativos no core)	Completar el levantamiento de todas las vulnerabilidades de los servidores y aplicativos core y no core de la institución educativa.	DI-ID-09
		La institución educativa cuenta con un procedimiento para la gestión de accesos para proveedores de las aplicaciones core, los cuales se encuentran operativos pero no están formalizados. Adicionalmente mediante el área de recursos humanos sí se cuenta con un proceso implementado para el cumplimiento de las claúsulas contractuales con el proveedor.	Levantar y definir una política para la gestión de seguridades cibernéticas con los proveedores.	DI-ID-10
PROTEGER (PR)	55%	La institución educativa cuenta con una política de seguridad de la información en la cual se define un proceso forma de acceso a los activos lógicos asociados a los sistemas core de la institución.	Incluir en el política de seguridad de la información de la institución educativa los procedimientos de acceso físico a la información.	DI-PR-01
		El área de seguridad de la información envía presentaciones correspondientes a la seguridad cibernética de forma periódica, capacitando a la comunidad de la institución educativa de los riesgos actuales.	Elaborar y formalizar un plan de capacitación y evaluaciones sobre temas de seguridad y ciberseguridad de la información en la institución educativa.	DI-PR-02
		La institución educativa cuenta con un proceso que asegura a la información que se encuentra en tránsito, sin embargo; no se cuenta con una gestión correspondiente a la información que se encuentra en reposo.	Diseñar e implementar un proceso que asegure a la información que se encuentra en reposo.	DI-PR-03
		La institución educativa cuenta con procedimientos para controlar la instalación del software en los sistemas operacionales.	Implementar un procedimiento formal para gestionar la protección de los sistemas de información y los activos.	DI-PR-04
		La institución educativa cuenta con un proceso informal para el mantenimiento y reparación de los componentes de los sistemas core. En modalidad remota se deberá acceder a los servidores mediante vpns.	Referirse a ID.AM.02	n/a
		La institución educativa cuenta con una política de seguridad de la información implementada en el antivirus, la cual restringe el uso de dispositivos externos, controlando de manera razonable la fuga de la información.	Establecer un procedimiento formal para el análisis y revisión de los logs identificados en el alcance de la evaluación de los aplicativos core y no core.	DI-PR-05
DETECTAR (DE)	69%	La institución educativa cuenta con herramienta LDP para el bloqueo del envío de información sensible y recepción de información sospechosa, dudosa procedencia. Adicionalmente se cuenta con la herramienta F5 que permite la detección de vulnerabilidades a nivel de IP's.	Diseñar e implementar una política para la gestión de incidentes conforme a la criticidad y asignación de prioridades para su resolución.	DI-DE-01
		La institución educativa realiza un proceso de monitoreo enfocada en la seguridad de la información pero no existen procesos para ciberseguridad.	Diseñar e implementar un proceso para monitorear los eventos de ciberseguridad.	DI-DE-02
		La institución educativa realiza un proceso de monitoreo enfocada en la seguridad de la información pero no existen procesos para ciberseguridad.	Referirse a DE.CM.01 Elaborar un proceso formal para difundir y comunicar los eventos de ciberseguridad.	n/a DI-DE-03
RESPONDER (RS)	59%	La institución educativa cuenta con un procedimiento para la atención y respuesta para los incidentes de seguridad de la información. No se han presentado incidentes de ciberseguridad en el último periodo.	Elaborar un proceso para la atención a incidentes de ciberseguridad.	DI-RS-01
		La institución educativa cuenta con un procedimiento para la comunicación de incidentes de seguridad de la información. No se han presentado incidentes de ciberseguridad en el último periodo.	Elaborar en el proceso de comunicación de incidentes de ciberseguridad.	DI-RS-02
		La institución educativa cuenta con un procedimiento para la comunicación de incidentes de seguridad de la información. No se han presentado incidentes de ciberseguridad en el último periodo.	Referirse a RS.RP.01	n/a
		La institución educativa cuenta con un procedimiento para la atención y respuesta para los incidentes de seguridad de la información. No se han presentado incidentes de ciberseguridad en el último periodo.	Referirse a RS.RP.01	n/a
RECUPERAR (RC)	53%	La institución educativa cuenta con un procedimiento para la recuperación y restauración de los sistemas o activos afectados por incidentes de seguridad de la información. No se han presentado incidentes de ciberseguridad en el último periodo.	Elaborar un procedimiento de recuperación para asegurar la restauración de los sistemas afectados por los incidentes de ciberseguridad que incluyan procedimientos de comunicación interna y externa.	DI-RC-01

Figura 5. Captura de pantalla del análisis realizado por cada categoría y la respectiva oportunidad de mejora.

2.3.2. Clasificación de Información

Para el análisis de clasificación de la información se identificaron las siguientes cuatro entidades:

- Alumnos
- Empleados
- Proveedores
- Organización

Sobre las cuales se identificaron el tipo de información que maneja cada una de ellas.

Tabla 2

Entidades identificadas

Entidad	Nombre del tipo de Información	Definición del tipo de información
ALUMNOS	Contacto/Ubicabilidad	Información de dirección, teléfonos, correos.
	Record académico	Información de materias tomadas (aprobadas y reprobada), convalidación, bachillerato, carrera que cursa (pregrado, postgrado, especializaciones), calificaciones.
	Salud	Discapacidad, enfermedad catastrófica, resultados de laboratorio (emo, copro, etc), enfermedades, historial de atención, persona de contacto.
	Financiera	Financiamientos, Beca (social, económica, deportiva), Estatus de morosidad.
	Personal	Nombres, apellidos, cargas, sexo, edad, orientación sexual, raza/etnia, tendencias políticas
EMPLEADOS	Contacto	Información de nombres, dirección, teléfonos, correos.
	Financiero	Certificados bancarios, nivel de endeudamiento.
	Salud	Discapacidad, enfermedad catastrófica, resultados de laboratorio (emo, copro, etc), enfermedades, historial de atención, persona de contacto.
	Ingresos	Sueldos, beneficios, bonos, comisiones, horas extras.

	Educación	Nivel educativo (básico, pregrado, postgrado).
	Personal	Nombres, apellidos, cargas, sexo, edad, orientación sexual, raza/etnia, tendencias políticas
	Legal	Juicio de alimentos, demandas.
PROVEEDORES	Contacto	Información de nombres, dirección, teléfonos, correos, persona natural, persona jurídica, estatus (vigente o cancelado).
	Tipo de servicio	Tecnológicos, administrativos, contable, limpieza, seguridad.
	Financiero	Valor contrato, forma de pago (mensual, trimestral), retenciones (si aplica o no).
	Calificación	Año de calificación, estatus de calificación.
ORGANIZACIÓN	Oferta académica	Post grados, Pregrados, Diplomados, especialidades, etc.
	Periodo académico	año, mes de ejecución de cada oferta académica
	Convenios	Bancos, universidades (investigación, pasantías), colegios, empresas.
	Financiero	Estados Financieros, facturas, N/C, N/D, tipos de financiamientos, presupuesto, costos.

Para el desarrollo del análisis de valoración de los activos, se tomó como referencia los siguientes rangos:

Tabla 3

Rangos de Valoración

1- Insignificante
2- Menor
3- Moderado
4- Mayor
5- Catastrófico

Adicionalmente se consideraron los parámetros de la tipología del modulador de riesgos, a continuación, el detalle.

- Pérdidas financieras.
- Interrupción de operaciones parciales y/o totales.
- Observaciones de auditoría interna o externas.
- Pérdida / Degradación de la Imagen institucional
- Demandas judiciales, afectación legal

Estos parámetros fueron evaluados y valorados, para todos los principios de la Seguridad de la Información, de las entidades de la institución educativa.

Principios de Seguridad de la Información:

- Disponibilidad
- Confidencialidad
- Privacidad
- Integridad

Entidad	Nombre del tipo de Información	Pérdidas financieras.	Interrupción de operaciones parciales y/o totales.	Observaciones de auditoría interna o externas.	Afectación al clima laboral.	Pérdida / Degradación de la Imagen	Demandas judicial, afectación Legal	Total	Perdida de confidencialidad
ALUMNOS	Contacto/Ubicabilidad	2	3	2	1	3	1	2	Menor
	Record académico	3	3	3	2	5	3	3	Mayor
	Salud	3	3	3	2	4	3	3	Moderado
	Financiera	1	1	1	1	1	1	1	Insignificante
	Personal	2	3	2	1	3	1	2	Menor
EMPLEADOS	Contacto	2	3	2	1	3	1	2	Menor
	Financiero	3	1	2	3	2	2	2	Moderado
	Salud	3	3	3	2	4	3	3	Moderado
	Ingresos	3	1	2	4	2	2	2	Moderado
	Educación	1	1	1	1	1	1	1	Insignificante
	Personal	2	3	2	1	3	1	2	Menor
	Legal	1	1	1	1	2	3	2	Menor

Figura 6. Ejemplo de valoración entidades: Alumnos y Empleados del principio de Confidencialidad.

Se obtuvo como resultado de la evaluación, que el tipo de información “Récord académico”, fue que el presenta un riesgo Catastrófico para la entidad educativa, y sobre el cual se seleccionó el activo crítico para el análisis de vulnerabilidades y amenazas.

Entidad	Nombre del tipo de Información	Definición del tipo de información	Pérdida de confidencialidad	Pérdida de privacidad	Pérdida de integridad	Pérdida de disponibilidad	Aplicativo	Tipo de activo	Clasificación de activo	Formato	Propietario	Proceso
ALUMNOS	Contacto/Ubicabilidad unificar con Personal	Información de dirección, teléfonos, correos.	Menor	Menor	Menor	Menor	Banner	Base de Datos Banner	Menor	Digital	Vicerrector académico	Matriculación
							Sistema de archivo	Reportes académicos estudiantes		Digital	Mentoría	Mentoría
	Récord académico	Información de materias tomadas (aprobadas y reprobada), convalidación, bachillerato, carrera que cursa (pregrado, postgrado, especializaciones), calificaciones.	Mayor	Catastrófico	Catastrófico	Mayor	Banner	Base de Datos Banner	Catastrófico	Digital	Vicerrector académico	Matriculación
							Sistema de archivo	Reportes académicos estudiantes		Digital	Mentoría	Mentoría
							CRM adminisiones	Reportes académicos		Digital	Director de	Admisiones
	Salud	Discapacidad, enfermedad castatrófica, resultados de laboratorio (emo, copro, etc), enfermedades, historial de atención, persona de contacto.	Moderado	Moderado	Menor	Moderado	Biodimed	Base de datos de biodimed	Moderado	Digital	Salud ocupacional	Salud ocupacional
							Sharepoint	Reporte		Digital	Mentoría	Mentoría
	Financiera	Financimientos, Beca (social, económica, deportiva), Estatus de morosidad.	Insignificante	Menor	Menor	Menor	Banner	Base de Datos Banner	Menor	Digital	Vicerrector académico	Matriculación
							Sharepoint	Reporte		Digital	Mentoría	Mentoría
	Personal	Nombres, apellidos, cargas, sexo, edad, orientación sexual, raza/etnia, tendencias políticas	Menor	Moderado	Moderado	Moderado	Banner	Base de Datos Banner	Moderado	Digital	Vicerrector académico	Matriculación
							Sharepoint	Reporte		Digital	Mentoría	Mentoría

Figura 7. Valoración del tipo de información por principios entidad alumnos”.

2.3.3. Inventarios de activos de Información

Para la identificación de activos de información, se tomó como base el tipo de información Récord Académico, cuya valoración fue Catastrófica en dos los principios de la Seguridad de la Información (Privacidad e Integridad).

Se identificaron los aplicativos, formatos, propietarios y procesos sobre los cuales se comparte este tipo de información, para identificar cuál activo es el crítico y sobre el cual se continuará con el análisis en las siguientes etapas.

Tabla 4

Inventario de activos críticos de información

Entidad	Nombre del tipo de Información	Definición del tipo de información	Aplicativo	Tipo de activo
ALUMNOS	Récord académico	Información de materias tomadas (aprobadas y reprobada), convalidación, bachillerato, carrera que cursa (pregrado, postgrado, especializaciones), calificaciones.	**Banner**	**Base de datos Banner**
			Banner	CarpetaEnLineaTutoriasWebApi
			Banner	Idea Survey Managment
			Banner	Identity Manager Api
			Banner	INT114- Servicio windows UdlaIntegracionesSAPWinServiceINT114
			Banner	INT123 - Servicio windows UdlaIntegracionesSAPWinServiceINT123
			Banner	Integración BX
			Banner	Servicio Workflow Request Status
			Banner	Servidor de App
			Banner	Servidor de comunicaciones
			Banner	Servidor de presentación web
			Banner	Servidor de reportes Cognos
			Banner	Sistema operativo
			Banner	Udla CommonWebApi

El activo de información seleccionado para el análisis es la Base de datos del aplicativo Banner, el mismo que soporta las transacciones de información correspondientes al proceso *core* de matriculación de los estudiantes de la entidad educativa.

Y sobre el cual se debe identificar las amenazas y vulnerabilidades a las cuales está expuesto.

2.3.4. Análisis de amenazas y vulnerabilidades de activos de información críticos

Tomando como base el estándar ISO 27001 y la metodología Magerit v3, se procedió a realizar la identificación de amenazas y vulnerabilidades para un activo crítico de información que en este caso es la base de datos del aplicativo Banner.

Se identificaron quince amenazas y veinticuatro vulnerabilidades, sobre las cuales se analizó si la entidad educativa mantiene algún tipo de control que pueda minimizar su riesgo.

El 66% de las vulnerabilidades carecen de control definido/aplicado por la institución educativa y sobre los cuales se propone un plan de acción.

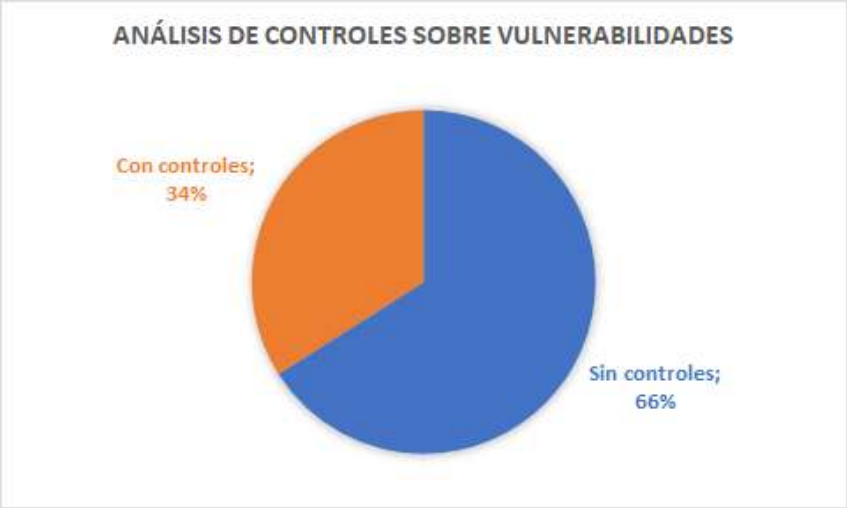


Figura 8. Análisis de controles sobre vulnerabilidades.

2.3.5. Documentos clave del SGSI

El desarrollo de esta fase comprende la definición de políticas de alto nivel que formarán parte del Sistema de Gestión de Seguridad de la Información (SGSI).

“Es importante indicar que una política de alto nivel o política general aborda la necesidad de la implementación de un sistema de gestión de seguridad de la información (SGSI) planteado desde la descripción del quién, qué, por qué, cuándo y cómo, en torno al desarrollo de la implementación del SGSI”. (MINTIC, 2016)

Como resultado de la ejecución de las fases anteriores, se definieron trece políticas de alto nivel las cuales se deben ser incluidas en el programa del SGI, las cuales se tomó como referencia ISO 27001.

A continuación, se detallan las políticas de alto nivel:

Tabla 5
Detalle políticas alto nivel.

Nombre	Responsable	Procesos
Política de Seguridad de la información.		
Política para la clasificación de activos de la información		

Política para el manejo de los activos de información.		
Política para asignación de Funciones y responsabilidades de seguridad de la información.		
Política para la asignación de recursos del SGSI.		
Política para evaluación de los riesgos de seguridad de la información.		Procesos Core del negocio:
Política para el tratamiento de los riesgos de seguridad de la Información	CISO	1. Académicos (Investigación, Asuntos regulatorios académicos, Evaluación y desarrollo del docente).
Política para la Concientización del SGSI		
Política para la Comunicación del SGSI		
Política para documentación de la información del SGSI.		
Políticas para efectuar Auditoría interna al SGSI.		2. Administrativos (Financieros, Admisiones y Operaciones, PMO).
Políticas para no conformidades del SGSI.		
Política para la mejora continua del SGSI		

2.3.6. Operación

El modelo operacional para el SGSI, se basa en el análisis de riesgos y la aplicación de controles en los procesos de la entidad educativa, toma las funciones del marco de referencia NIST de ciberseguridad.

Se definieron métricas para el seguimiento y el cumplimiento de este modelo, las cuales se plantearon para el primer y segundo año, como se muestra a continuación:

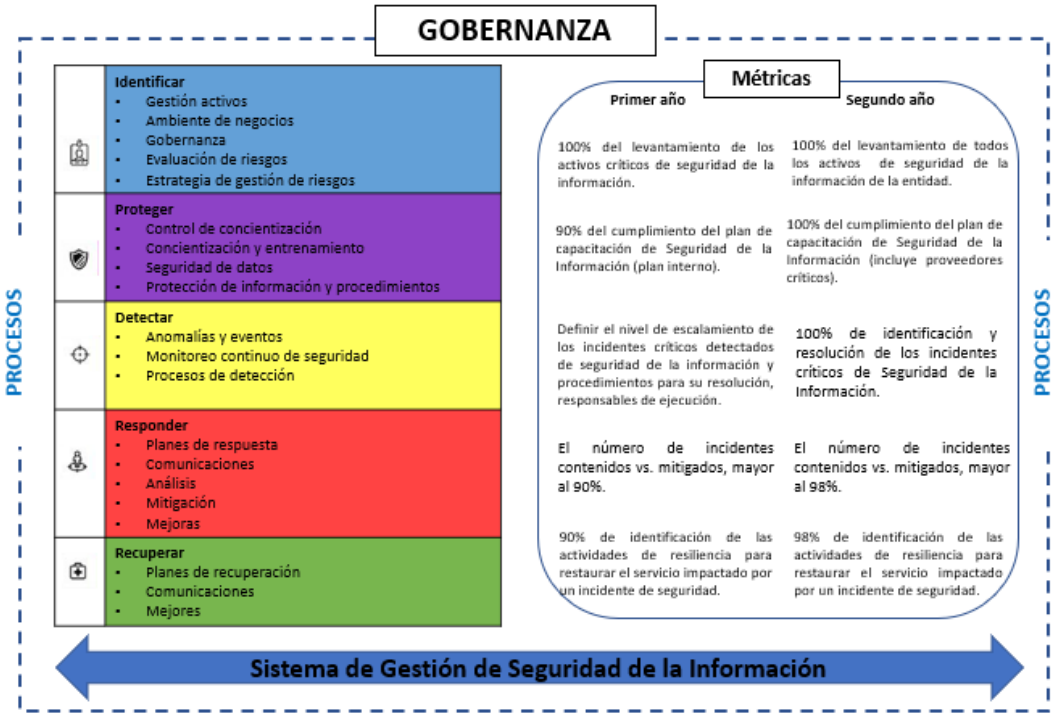


Figura 9. Modelo operacional

2.3.7. Programa del SGSI

El programa del SGSI, cuenta con cuarenta y siete actividades, las cuales han sido planificadas para ejecutarse durante el año 2022, cada actividad cuenta con un responsable asignado, y se ha definido el área a la cual impactará dicha actividad.

Las actividades han sido codificadas conforme la fase teniendo así:

Tabla 6

Codificación de las actividades

Sufijos	Fase
DI	Diagnóstico inicial
CI	Clasificación de la información
IA	Inventario de activos
AI	Activos de Información
DC	Documentos clave

Tabla 7

Actividades para desarrollar generadas de la fase “Diagnóstico Inicial”

Cod.	Actividad
DI-ID-01	Establecer proceso de evaluación de los riesgos de seguridad de la información, para identificar los riesgos asociados a la pérdida de la confidencialidad, integridad y disponibilidad de la información.
DI-ID-02	Realizar el levantamiento y clasificación de los activos de información críticos según el tipo de información.
DI-ID-03	Definir métricas que permitan medir el cumplimiento de la normativa interna respecto de seguridad de la información.
DI-ID-04	Definir, coordinar, aprobar objetivos y requisitos de seguridad de la información dentro de la arquitectura de la institución.
DI-ID-05	Documentar los controles de seguridad de la información que mantiene la institución e implementar escenarios y actividades de resiliencia para respuesta de ataques internos.
DI-ID-06	Analizar, evaluar y formalizar normativa para ciberseguridad en la institución.
DI-ID-07	Analizar, evaluar y formalizar normativa para el gobierno de ciberseguridad en la institución educativa.
DI-ID-08	Analizar, evaluar y formalizar normativa para la evaluación de riesgos de ciberseguridad en la institución educativa.
DI-ID-09	Completar el levantamiento de todas las vulnerabilidades de los servidores y aplicativos core y no core de la institución educativa.
DI-ID-10	Levantar y definir una política para la gestión de seguridades cibernéticas con los proveedores.

DI-PR-01	Incluir en la política de seguridad de la información de la institución educativa los procedimientos de acceso físico a la información.
DI-PR-02	Elaborar y formalizar un plan de capacitación y evaluaciones sobre temas de seguridad y ciberseguridad de la información en la institución educativa.
DI-PR-03	Diseñar e implementar un proceso que asegure a la información que se encuentra en reposo.
DI-PR-04	Implementar un procedimiento formal para gestionar la protección de los sistemas de información y los activos.
DI-PR-05	Establecer un procedimiento formal para el análisis y revisión de los logs identificados en el alcance de la evaluación de los aplicativos core y no core.
DI-DE-01	Diseñar e implementar una política para la gestión de incidentes conforme a la criticidad y asignación de prioridades para su resolución.
DI-DE-02	Diseñar e implementar un proceso para monitorear los eventos de ciberseguridad.
DI-DE-03	Elaborar un proceso formal para difundir y comunicar los eventos e incidentes de ciberseguridad.
DI-RS-01	Elaborar un proceso para la atención a incidentes de ciberseguridad.
DI-RC-01	Elaborar un procedimiento de recuperación para asegurar la restauración de los sistemas afectados por los incidentes de ciberseguridad que incluyan procedimientos de comunicación interna y externa.

Tabla 8

Actividades para desarrollar generadas de la fase “Documentos Clave”

Cod.	Actividad
DC-PO-01	Actualizar la Política de Seguridad de la información.
DC-PO-02	Política para la clasificación de activos de la información
DC-PO-03	Política para el manejo de los activos de información.
DC-PO-04	Política para asignación de Funciones y responsabilidades de seguridad de la información.
DC-PO-05	Política para la asignación de recursos del SGSI.
DC-PO-06	Política para evaluación de los riesgos de seguridad de la información.
DC-PO-07	Política para el tratamiento de los riesgos de seguridad de la Información

DC-PO-08	Política para la Concientización del SGSI
DC-PO-09	Política para la Comunicación del SGSI
DC-PO-10	Política para documentación de la información del SGSI.
DC-PO-11	Políticas para efectuar Auditoría interna al SGSI.
DC-PO-12	Políticas para no conformidades del SGSI.
DC-PO-13	Política para la mejora contínua del SGSI

Tabla 9

Actividades para desarrollar generadas de la fase “Activos de Información”

Cod.	Actividad
AI-CT-02	Coordinar con el área de Recursos Humanos y Legal para incluir en los contratos con los proveedores las adendas que contengan parámetros mínimos de seguridad de la información que deben implementar y seguir los proveedores.
AI-CT-03	Definir e implementar un plan y cronograma de capacitaciones al personal administrador de base de datos.
AI-CT-04	Definir e implementar un procedimiento que norme la asignación de parámetros para monitorear los incidentes de seguridad en las bases de datos, en la cual se detalle el responsable, la periodicidad y soporte de la ejecución.
AI-CT-05	Definir e implementar un procedimiento que norme los controles para efectuar los cambio en las configuraciones de la base de datos, en la cual se detalle el responsable, la periodicidad y soporte de la ejecución.
AI-CT-06	Definir e implementar un procedimiento que norme los controles para monitorear los derechos de acceso de los administradores, en la cual se detalle el responsable, la periodicidad y soporte de la ejecución.
AI-CT-07	Diseñar e implementar un procedimiento que permita realizar un control periódico de los accesos sensitivos a usuarios que tienen acceso a las aplicaciones, en la cual se detalle el responsable, la periodicidad y soporte de la ejecución.
AI-CT-08	Elaborar un manual de usuario que detalle el correcto uso de la interfaz.
AI-CT-09	Elaborar un procedimiento que genere reportes de fallas en los registros de administradores y operadores, en la cual se detalle el responsable, la periodicidad y soporte de la ejecución.

AI-CT-10	Elaborar un procedimiento que supervise al personal externo o de limpieza que tienen acceso a información sensitiva, en la cual se detalle el responsable, la periodicidad y soporte de la ejecución.
AI-CT-11	Elaborar un procedimiento que supervise los derechos de acceso sobre los usuarios activos con permisos sensitivos, en la cual se detalle el responsable, la periodicidad y soporte de la ejecución.
AI-CT-12	Implementar controles de monitoreo y revisión de los roles de acceso que se mantienen a las bases de datos.
AI-CT-13	Implementar herramientas automáticas de detección de transacciones sensitivas en las bases de datos.
AI-CT-14	Implementar herramientas para el registro de pistas de auditoría (logs) en base de datos.
AI-CT-15	Incluir dentro de la estructura de la seguridad de la información las funciones y personal responsable de su ejecución.

Para ver a mayor detalle las actividades del programa del SGSI, ver Anexo 2.

3. CONCLUSIONES Y RECOMENDACIONES

3.1 Conclusiones:

La institución educativa mantiene procesos y controles operativos para la gestión de seguridad de la información, el análisis realizado conforme el marco de referencia NIST, refleja la situación actual sobre el ambiente de control de sus activos críticos de información:

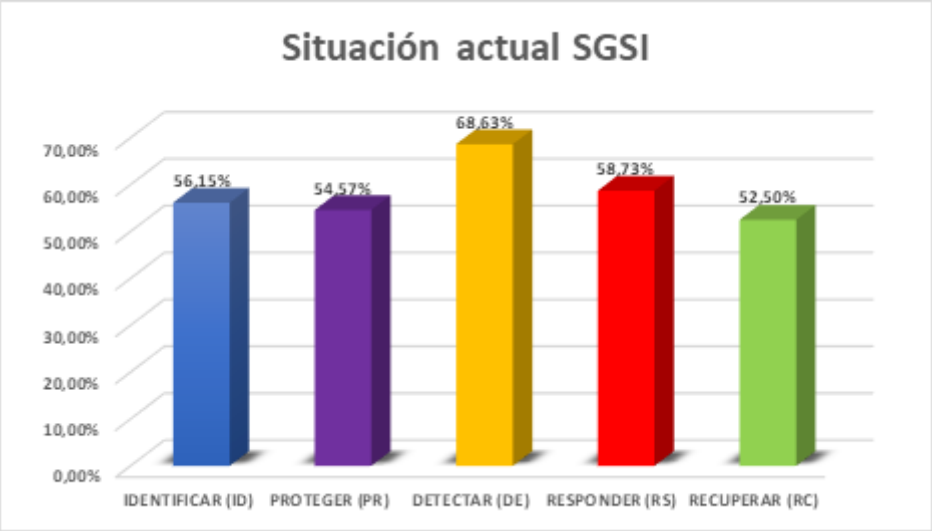


Figura 10. Situación actual institución educativa.

El rango de cumplimiento está entre el 52% y 58%, en cuatro de las cinco funciones de NIST, la institución educativa ha invertido mayor esfuerzo y presenta un mayor nivel de cumplimiento en la fase de “Detectar” con un 68%

Si bien la institución educativa ha realizado esfuerzos importantes, incluso incluye dentro de sus objetivos estratégicos de la institución la arquitectura, procesos y controles sobre la seguridad de la información, es importante que se consideren riesgos, procesos y controles para una seguridad cibernética.

Por lo cual, el trabajo efectuado en este proyecto de titulación ratifica la necesidad de implementar y formalizar un Modelo operacional del SGSI.

3.2 Recomendaciones:

- Establecer y formalizar una metodología, para gestionar la seguridad de la información y ciberseguridad, con el fin de alinear los parámetros de las buenas prácticas de forma clara y concisa.

- La institución educativa debe formalizar la gestión continua de riesgos sobre Seguridad de la Información y Ciberseguridad, incluyendo la aplicación de controles y monitoreo continuo para que su ejecución sea efectiva.

- La institución educativa debe establecer políticas de comunicación interna efectivas, para inculcar a la comunidad educativa las mejores prácticas sobre Seguridad de la Información y Ciberseguridad, y los riesgos a los que está expuesta si los mismos llegan a materializarse.

4. REFENCIAS

GlobalSUITE. (2018). ¿Qué es NIST Cibersecurity Framework? Recuperado el 1 de julio de 2021 de https://www.globalsuitesolutions.com/es/que-es-nist-cibersecurity-framework/

ISACA. (2020). COBIT Focus Area: Information Security. 194 páginas.

Ministerio de Tecnologías de la Información y Comunicaciones de Colombia. (2016) 25 páginas. Elaboración de la política general de seguridad y privacidad de la información.

It ahora. (2020) Deloitte, AECI, OEA. 18 páginas. Estado Actual de la Ciberseguridad 2020.

Expansión México. (2020) Tecnología. Recuperado el 2 septiembre de 2021 de https://expansion.mx/tecnologia/2020/08/26/las-universidades-en-jaque-informatico

5. ANEXOS

Anexo 1 Valoración de la entidad educativa según NIST

Función	Categoría	Subcategoría	Referencias informativas	COBIT 2019- Actividades	Autoevaluacion	Promedio
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 objetivos organizativos y la estrategia de riesgos de la organización.	**ID.AM-1:** Los dispositivos y sistemas físicos dentro de la organización están inventariados.	**COBIT 5** BAI09.01	1. Visualice y documente los activos de I&T de la empresa para incluir el flujo de datos.	60%	44%
				2. Identificar los requisitos de seguridad de la información para los activos actuales.	50%	
				3. Abordar la seguridad de la información para activos, datos y formularios de I&T, etc.	10%	
				4. Verificar que un inventario de activos completo y preciso informa la implementación de los procesos de seguridad (gestión parches, gestión de vulnerabilidades, etc.). Orientación relacionada (estándares, marcos, cumplimiento)	30%	
			COBIT 5 BAI09.02	1. Defina los niveles de criticidad e identifique la criticidad de los activos en un registro de activos.	10%	
				2. Hacer cumplir los requisitos de seguridad de la información en los activos.	80%	
				3. Incluir medidas de seguridad (p. Ej., Revisiones de seguridad del centro de datos) que aborden el acceso de terceros a las instalaciones de I&T de la empresa para el sitio y actividades fuera del sitio. Garantizar las condiciones adecuadas de seguridad y privacidad, especialmente en el contexto de la subcontratación.	100%	
				4. Asegúrese de que la clasificación de seguridad de los datos esté incorporada en el inventario de activos.	10%	
		ID.AM-2: Las plataformas de software y las aplicaciones dentro de la organización están inventariadas.	**COBIT 5** BAI09.05	1. Establecer un procedimiento para el control de las instalaciones de software y otros activos de I&T.	100%	60%
				2. Realice comprobaciones periódicas de la red en busca de software no autorizado.	20%	
		ID.AM-4: Los sistemas de información externos están catalogados.	**COBIT 5** APO02.02	1. Desarrollar una línea base de capacidad de seguridad de la información.	100%	74%
				2. Crear criterios de seguridad de la información claros y relevantes para identificar riesgos y priorizar brechas.	100%	
			COBIT 5 APO10.04	1. Evaluar periódicamente los perfiles de riesgo de los proveedores en función de las necesidades y requisitos de seguridad de la información.	60%	
			COBIT 5 DSS01.02	1. Incorporar requisitos de seguridad de la información en los contratos.	100%	
				2. Supervise activamente el cumplimiento de terceros con las políticas, los estándares y los requisitos de seguridad de la información empresarial.	10%	
		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.	**COBIT 5** APO03.03	1. Asegurar la inclusión de los requisitos de seguridad de la información al analizar las brechas y seleccionar soluciones para la empresa.	70%	42%
				2. Proporcionar un inventario detallado de la información y los activos físicos con la clasificación, propiedad, ubicación y mantenimiento adecuados. tipo, valor y criticidad .	60%	
			COBIT 5 APO03.04	1. Alinee la seguridad de la información con la arquitectura de I&T.	70%	
			COBIT 5 APO12.01	1. Identificar y recopilar datos relevantes para permitir la identificación, el análisis y la generación de informes de riesgos relacionados con la seguridad de la información.	30%	
			COBIT 5 BAI04.02	1. Evalúe el impacto en la seguridad de la información de la posible falta de disponibilidad, bajo rendimiento y falta de capacidad.	50%	
				2. Evaluar el impacto comercial de la falta de disponibilidad potencial, el bajo rendimiento y la falta de capacidad debido a la introducción de controles de seguridad de la información .	10%	
				3. Evaluar el impacto comercial de la posible indisponibilidad, el bajo rendimiento y la falta de capacidad debido a una posible información incidente de seguridad .	10%	
			COBIT 5 BAI09.02	1. Define criticality levels and identify asset criticality in an asset register.	10%	
				2. Enforce information security requirements on assets.	80%	
				3. Include security measures (e.g., data center security reviews) that address third-party access to enterprise I&T facilities for onsite and off-site activities. Ensure appropriate security and privacy conditions, especially in the context of outsourcing.	65%	
				4. Ensure that the security classification of data is embedded in the asset inventory.	10%	
		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.	**COBIT 5** APO01.02	1. Define the expectations with regard to information security, including specific organizational ethics and culture.	80%	67%
				2. Develop an information security awareness program.	50%	
				3. Establish metrics to measure behaviors regarding information security. Related Guidance (Standards, Frameworks, Compliance Requirements)	60%	
			COBIT 5 APO07.06	1. Obtain formal agreement from contract staff on information security policies and requirements.	80%	
				2. Establish formal policies and procedures for contract staff.	50%	
			COBIT 5 DSS06.03	1. Allocate access rights on the basis of need-to-know and least-privilege principles and job requirements.	70%	
				2. Periodically review authorizations.	80%	

Función	Categoría	Subcategoría	Referencias informativas	COBIT 2019- Actividades	Autoevaluacion	Promedio
IDENTIFICAR (ID)	**Entorno empresarial (ID.BE): Se entienden y se priorizan la misión, los objetivos, las partes interesadas y las actividades de la organización; esta información se utiliza para informar los roles, responsabilidades y decisiones de gestión de los riesgos de seguridad cibernética.**	**ID.BE-1:** Se identifica y se comunica la función de la organización en la cadena de suministro.	**COBIT 5** APO08.01	1. Understand the business and how information security enables/affects it.	60%	**75%**
			COBIT 5 APO08.04	1. Establish appropriate communication channels between the information security function and the business.	100%	
				2. Establish appropriate reporting and metrics regarding information security.	70%	
			COBIT 5 APO08.05	1. Incorporate information security requirements in the continual improvement process.	80%	
			COBIT 5 APO10.04	1. Periodically reassess supplier risk profiles based on information security needs and requirements.	60%	
			COBIT 5 APO10.05	1. Review vendor information security performance.	80%	
		ID.BE-2: Se identifica y se comunica el lugar de la organización en la infraestructura crítica y su sector industrial.	**COBIT 5** APO02.06	1. Promote the information security function.	40%	**65%**
				2. Develop the information security plan/program, outlining the practical consequences of information security for the enterprise.	50%	
				3. Communicate the information security strategy and information security plan/program to the enterprise and all relevant stakeholders.	80%	
			COBIT 5 APO03.01	1. Define information security objectives and requirements for the enterprise architecture.	10%	
				2. Consider industry best practices in building the information security architecture vision.	90%	
				3. Ensure inclusion of information security requirements when analyzing gaps and selecting solutions for the enterprise.	100%	
				4. Define the information security goals and metrics.	100%	
				5. Incorporate defense-in-depth strategies in the enterprise security architecture.	50%	
		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	1. Understand how information security should support overall enterprise objectives and protect stakeholder interests by taking into account the need to manage information risk while meeting legal and regulatory compliance requirements.	100%	**74%**
				2. Understand the current enterprise architecture and identify potential information security gaps.	90%	
			COBIT 5 APO02.06	1. Promote the information security function.	80%	
				2. Develop the information security plan/program, outlining the practical consequences of information security for the enterprise	40%	
				3. Communicate the information security strategy and information security plan/program to the enterprise and all relevant stakeholders.	80%	
			COBIT 5 APO03.01	1. Define information security objectives and requirements for the enterprise architecture. 2	10%	
				2. Consider industry best practices in building the information security architecture vision.	90%	
				3. Ensure inclusion of information security requirements when analyzing gaps and selecting solutions for the enterprise.	100%	
				4. Define the information security goals and metrics.	100%	
				5. Incorporate defense-in-depth strategies in the enterprise security architecture.	50%	
		ID.BE-4: Se establecen las dependencias y funciones fundamentales para la entrega de servicios críticos.	**COBIT 5** APO10.01	1. Conduct information risk assessments and define the information risk profile. 3	40%	**57%**
				2. Define the supplier relationship and requirements based on the information risk profile.	60%	
			COBIT 5 BAI04.02	1. Assess the information security impact of potential unavailability, underperformance and lack of capacity. 4	70%	
				2. Assess the business impact of potential unavailability, underperformance and lack of capacity due to introduction of information security controls.	70%	
				3. Assess the business impact of potential unavailability, underperformance and lack of capacity due to a potential information security incident.	70%	
			COBIT 5 BAI09.02	1. Define criticality levels and identify asset criticality in an asset register. 2	10%	
				2. Enforce information security requirements on assets. 3	80%	
				3. Include security measures (e.g., data center security reviews) that address third-party access to enterprise I&T facilities for onsite and off-site activities. Ensure appropriate security and privacy conditions, especially in the context of outsourcing.	100%	
				4. Ensure that the security classification of data is embedded in the asset inventory	10%	
		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).	**COBIT 5** BAI03.02	1. Integrate information security design into solution components.	70%	**55%**
			COBIT 5 DSS04.02	1. Include information security scenarios in business resilience activities.	40%	

Función	Categoría	Subcategoría	Referencias informativas	COBIT 2019- Actividades	Autoevaluacion	Promedio
IDENTIFICAR (ID)	**Gobernanza (ID.GV):** Las políticas, los procedimientos y 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-1:** Se establece y se comunica la política de seguridad cibernética organizacional.	**COBIT 5** EDM01.01	1. Analyze and identify the internal and external environmental factors (legal, regulatory and contractual obligations) and trends in the business environment that may influence the information security governance design.	40%	**40%**
				2. Evaluate the extent to which information security meets business and compliance/regulatory needs.	40%	
				3. Articulate principles that will guide the design of information security and promote a security-positive environment.	40%	
				4. Understand the enterprise's decision-making culture and determine the optimal decision-making model for information security.	40%	
				5. Understand the enterprise's training program to promote a governance structure and environment. 3	40%	
				6. Evaluate the extent to which information security is aligned to legal and regulatory trends.	40%	
		ID.GV-2: Los roles y las responsabilidades de seguridad cibernética están coordinados y alineados con roles internos y socios externos.	**COBIT 5** APO01.02	1. Define the expectations with regard to information security, including specific organizational ethics and culture.	80%	**63%**
				2. Develop an information security awareness program.	50%	
				3. Establish metrics to measure behaviors regarding information security.	60%	
		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.	**COBIT 5** BAI02.01	1. Research, define and document information security requirements (i.e., confidentiality requirements, integrity requirements and availability requirements)	90%	**73%**
				2. Research and analyze information security requirements with stakeholders, business sponsors and technical implementation personnel.	60%	
				3. Ensure that the business functional requirements take into account the need to protect the security of information (e.g., detect and prevent fraud, validate customer identity).	90%	
				4. Ensure that the technical requirements take into account the need to protect the security of information (e.g., data storage and encryption requirements, hardening of servers, architecture design, penetration tests).	70%	
			COBIT 5 MEA03.01	1. Establish arrangements for monitoring information security compliance to external requirements. 2	70%	
				2. Determine external compliance requirements to be met (including legal, regulatory, privacy and contractual requirements).	70%	
				3. Identify and communicate sources of information security material to help meet external compliance requirements.	50%	
			COBIT 5 MEA03.04	1. In the absence of third-party assurance, obtain evidence of compliance from third parties.	80%	
		ID.GV-4: Los procesos de gobernanza y gestión de riesgos abordan los riesgos de seguridad cibernética.	**COBIT 5** DSS04.02	1. Include information security scenarios in business resilience activities.	40%	**40%**

Función	Categoría	Subcategoría	Referencias informativas	COBIT 2019- Actividades	Autoevaluacion	Promedio
IDENTIFICAR (ID)	**Evaluación de riesgos (ID.RA):** La organización comprende el 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-1:** Se identifican y se documentan las vulnerabilidades de los activos.	**COBIT 5** APO12.01	1. Identify and collect relevant data to enable effective information security-related risk identification, analysis and reporting.	30%	**68%**
			COBIT 5 APO12.03	1. Incorporate information security in the enterprise risk profile.	90%	
			COBIT 5 DSS05.01	1. Ensure that a vulnerability management program, including patch and configuration management, is in place.	90%	
				2. Ensure that antivirus, appropriate sandboxing and other advanced threat protection (ATP) measures are selected, deployed, monitored and maintained.	60%	
		ID.RA-3: Se identifican y se documentan las amenazas, tanto internas como externas.	**COBIT 5** APO12.01	1. Identify and collect relevant data to enable effective information security-related risk identification, analysis and reporting.	30%	**60%**
			COBIT 5 APO12.03	1. Incorporate information security in the enterprise risk profile.	90%	
		ID.RA-4: Se identifican los impactos y las probabilidades del negocio.	**COBIT 5** DSS04.02	1. Include information security scenarios in business resilience activities.	40%	**40%**
	Estrategia de gestión de riesgos (ID.RM): Se establecen las prioridades, restricciones, tolerancias de riesgo y suposiciones de la organización y se usan para respaldar las decisiones de riesgos operacionales.	**ID.RM-1:** Los actores de la organización establecen, gestionan y acuerdan los procesos de gestión de riesgos.	**COBIT 5** BAI02.03	1. Identify the information security controls.	60%	**30%**
			COBIT 5 BAI04.02	1. Assess the information security impact of potential unavailability, underperformance and lack of capacity.	20%	
				2. Assess the business impact of potential unavailability, underperformance and lack of capacity due to introduction of information security controls.	20%	
				3. Assess the business impact of potential unavailability, underperformance and lack of capacity due to a potential information security incident.	20%	
		ID.RM-2: La tolerancia al riesgo organizacional se determina y se expresa claramente.	**COBIT 5** APO12.06	1. Apply selected information security mitigation practices.	80%	**80%**

Función	Categoría	Subcategoría	Referencias informativas	COBIT 2019- Actividades	Autoevaluacion	Promedio
IDENTIFICAR (ID)	**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 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.	**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.	**COBIT 5** APO10.01	1. Conduct information risk assessments and define the information risk profile.	40%	**61%**
				2. Define the supplier relationship and requirements based on the information risk	60%	
			COBIT 5 APO10.04	1. Periodically reassess supplier risk profiles based on information security needs and requirements.	60%	
			COBIT 5 BAI02.03	1. Identify the information security controls.	60%	
			COBIT 5 BAI04.02	1. Assess the information security impact of potential unavailability, underperformance and lack of capacity.	70%	
				2. Assess the business impact of potential unavailability, underperformance and lack of capacity due to introduction of information security controls.	70%	
				3. Assess the business impact of potential unavailability, underperformance and lack of capacity due to a potential information security incident.	70%	
		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 evaluación de riesgos de la cadena de suministro cibernético.	**COBIT 5** APO10.01	1. Conduct information risk assessments and define the information risk profile.	40%	**51%**
				2. Define the supplier relationship and requirements based on the information risk profile.	60%	
			COBIT 5 APO10.04	1. Periodically reassess supplier risk profiles based on information security needs and requirements.	60%	
			COBIT 5 APO10.05	1. Review vendor information security performance.	10%	
			COBIT 5 APO12.01	1. Identify and collect relevant data to enable effective information security-related risk identification, analysis and reporting.	10%	
			COBIT 5 APO12.03	1. Incorporate information security in the enterprise risk profile.	90%	
			COBIT 5 APO12.06	1. Apply selected information security mitigation practices.	80%	
			COBIT 5 BAI02.03	1. Identify the information security controls.	60%	
		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.	**COBIT 5** APO10.01	1. Conduct information risk assessments and define the information risk profile.	40%	**43%**
				2. Define the supplier relationship and requirements based on the information risk profile.	60%	
			COBIT 5 APO10.04	1. Periodically reassess supplier risk profiles based on information security needs and requirements.	60%	
			COBIT 5 APO10.05	1. Review vendor information security performance.	10%	
		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.	**COBIT 5** APO10.01	1. Conduct information risk assessments and define the information risk profile.	40%	**43%**
				2. Define the supplier relationship and requirements based on the information risk profile.	60%	
			COBIT 5 APO10.04	1. Periodically reassess supplier risk profiles based on information security needs and requirements.	60%	
			COBIT 5 APO10.05	1. Review vendor information security performance.	10%	
			COBIT 5 MEA01.02	1. Define information security performance targets consistent with overall I&T performance standards.	20%	
				2. Communicate information security performance and conformance targets with key due diligence stakeholders.	80%	
				3. Evaluate whether the information security goals and metrics are adequate: specific, measurable, achievable, relevant and timebound.	20%	
			COBIT 5 MEA01.03	1. Collect and analyze performance and conformance data relating to information security and information risk management (e.g., information security metrics, information security reports).	30%	
			COBIT 5 MEA01.04	1. Design, implement and agree on a range of information security performance reports.	60%	
			COBIT 5 MEA01.05	1. Develop a tracking process for corrective actions on information security issues.	50%	

Función	Categoría	Subcategoría	Referencias informativas	COBIT 2019- Actividades	Autoevaluacion	Promedio
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 autorizadas y transacciones.	**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.	**COBIT 5** DSS06.03	1. Allocate access rights on the basis of need-to-know and least-privilege principles and job requirements.	70%	**75%**
				2. Periodically review authorizations.	80%	
		PR.AC-2: Se gestiona y se protege el acceso físico a los activos.	**COBIT 5** DSS01.04	1. Ensure that environmental management adheres to information security requirements.	50%	**50%**
		PR.AC-3: Se gestiona el acceso remoto.	**COBIT 5** DSS01.04	1. Ensure that environmental management adheres to information security requirements.	50%	**50%**
		PR.AC-5: Se protege la integridad de la red (por ejemplo, segregación de la red, segmentación de la red).	**COBIT 5** DSS01.05	1. Ensure that facilities management adheres to information security requirements.	80%	**80%**
		PR.AC-6: Las identidades son verificadas y vinculadas a credenciales y afirmadas en las interacciones	**COBIT 5** DSS06.03	1. Allocate access rights on the basis of need-to-know and least-privilege principles and job requirements.	70%	**75%**
				2. Periodically review authorizations.	80%	
	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 conformidad con las políticas, los procedimientos y los acuerdos relacionados al campo.	**PR.AT-1:** Todos los usuarios están informados y capacitados.	**COBIT 5** APO07.03	1. Obtain formal agreement from staff on information security policies and requirements.	10%	**36%**
				2. Provide professional development training and programs on information security.	40%	
				3. Use credentialing to augment a quality information security professional skill set.	60%	
				4. Establish appropriate enterprisewide education, training and awareness programs for information security.	40%	
			COBIT 5 BAI05.07	1. Inform and train staff at periodic intervals based on information security needs.	30%	
		PR.AT-2: Los usuarios privilegiados comprenden sus roles y responsabilidades.	**COBIT 5** APO07.02	1. Ensure segregation of duties (SoD) in critical positions.	90%	**80%**
			COBIT 5 DSS06.03	1. Allocate access rights on the basis of need-to-know and least-privilege principles and job requirements.	70%	
				2. Periodically review authorizations.	80%	
		PR.AT-3: Los terceros interesados (por ejemplo, proveedores, clientes, socios) comprenden sus roles y responsabilidades.	**COBIT 5** APO07.03	1. Obtain formal agreement from staff on information security policies and requirements.	10%	**40%**
				2. Provide professional development training and programs on information security.	40%	
				3. Use credentialing to augment a quality information security professional skill set.	60%	
				4. Establish appropriate enterprisewide education, training and awareness programs for information security.	40%	
			COBIT 5 APO07.06	1. Obtain formal agreement from contract staff on information security policies and requirements.	50%	
				2. Establish formal policies and procedures for contract staff.	50%	
			COBIT 5 APO10.04	1. Periodically reassess supplier risk profiles based on information security needs and requirements.	60%	
			COBIT 5 APO10.05	1. Review vendor information security performance.	10%	
		PR.AT-4: Los ejecutivos superiores comprenden sus roles y responsabilidades.	**COBIT 5** EDM01.01	1. Analyze and identify the internal and external environmental factors (legal, regulatory and contractual obligations) and trends in the business environment that may influence the information security governance design.	40%	**45%**
				2. Evaluate the extent to which information security meets business and compliance/regulatory needs.	40%	
				3. Articulate principles that will guide the design of information security and promote a security-positive environment.	40%	
				4. Understand the enterprise's decision-making culture and determine the optimal decision-making model for information security.	40%	
				5. Understand the enterprise's training program to promote a governance structure and environment. 3	40%	
				6. Evaluate the extent to which information security is aligned to legal and regulatory trends.	40%	
			COBIT 5 APO01.02	1. Define the expectations with regard to information security, including specific organizational ethics and culture.	80%	
				2. Develop an information security awareness program.	50%	
				3. Establish metrics to measure behaviors regarding information security.	60%	
			COBIT 5 APO07.03	1. Obtain formal agreement from staff on information security policies and requirements.	10%	
				2. Provide professional development training and programs on information security.	40%	
				3. Use credentialing to augment a quality information security professional skill set.	60%	
				4. Establish appropriate enterprisewide education, training and awareness programs for information security.	40%	
		PR.AT-5: El personal de seguridad física y cibernética comprende sus roles y responsabilidades.	**COBIT 5** APO07.03	1. Obtain formal agreement from staff on information security policies and requirements.	10%	**38%**
				2. Provide professional development training and programs on information security.	40%	
				3. Use credentialing to augment a quality information security professional skill set.	60%	
				4. Establish appropriate enterprisewide education, training and awareness programs for information security.	40%	

Función	Categoría	Subcategoría	Referencias informativas	COBIT 2019- Actividades	Autoevaluacion	Promedio
PROTEGER (PR)	**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.	**COBIT 5** APO01.06	1. Define the information security function and all relevant activities and attributes.	60%	**54%**
				2. Define the placement of the information security function in the enterprise and obtain agreement from all relevant parties	70%	
			COBIT 5 BAI02.01	1. Research, define and document information security requirements (i.e., confidentiality requirements, integrity requirements and availability requirements)	10%	
				2. Research and analyze information security requirements with stakeholders, business sponsors and technical implementation personnel.	60%	
				3. Ensure that the business functional requirements take into account the need to protect the security of information (e.g., detect and prevent fraud, validate customer identity).	90%	
				4. Ensure that the technical requirements take into account the need to protect the security of information (e.g., data storage and encryption requirements, hardening of servers, architecture design, penetration tests).	70%	
			COBIT 5 BAI06.01	1. Ensure that the information security policy adapts to business goals within an enterprise.	50%	
				2. Ensure that changes conform with the information security policy.	20%	
				3. Ensure that assessment of the potential impact of changes on information security is undertaken.	10%	
				4. Develop practices to consider the information security impact of emerging trends and technologies.	40%	
			COBIT 5 DSS04.07	1. Ensure that information security requirements are included in the backup and restore arrangements.	100%	
			COBIT 5 DSS06.06	1. Enforce data classification, acceptable use, and information security policies and procedures to support information asset protection.	70%	
		PR.DS-2: Los datos en tránsito están protegidos.	**COBIT 5** APO01.06	1. Define the information security function and all relevant activities and attributes.	60%	**67%**
				2. Define the placement of the information security function in the enterprise and obtain agreement from all relevant parties.	70%	
			COBIT 5 DSS06.06	1. Enforce data classification, acceptable use, and information security policies and procedures to support information asset protection.	70%	
		PR.DS-3: Los activos se gestionan formalmente durante la eliminación, las transferencias y la disposición.	**COBIT 5** BAI09.03	1. Identify and communicate the risk of information security noncompliance related to the asset life cycle.	30%	**50%**
				2. Ensure that information security measures and requirements are met throughout the asset life cycle.	70%	
				3. Identify end-of-life systems and plan for related information security risk.	40%	
		PR.DS-5: Se implementan protecciones contra las filtraciones de datos.	**COBIT 5** APO01.06	1. Define the information security function and all relevant activities and attributes.	60%	**65%**
				2. Define the placement of the information security function in the enterprise and obtain agreement from all relevant parties.	70%	
		PR.DS-6: Se utilizan mecanismos de comprobación de la integridad para verificar el software, el firmware y la integridad de la información.	**COBIT 5** APO01.06	1. Define the information security function and all relevant activities and attributes.	60%	**42%**
				2. Define the placement of the information security function in the enterprise and obtain agreement from all relevant parties.	70%	
			COBIT 5 BAI06.01	1. Ensure that the information security policy adapts to business goals within an enterprise.	50%	
				2. Ensure that changes conform with the information security policy.	20%	
				3. Ensure that assessment of the potential impact of changes on information security is undertaken.	10%	
				4. Develop practices to consider the information security impact of emerging trends and technologies.	40%	
		PR.DS-7: Los entornos de desarrollo y prueba(s) están separados del entorno de producción.	**COBIT 5** BAI03.08	1. Validate that information security features match information security requirements.	50%	**50%**
		PR.DS-8: Se utilizan mecanismos de comprobación de la integridad para verificar la integridad del hardware.	**COBIT 5** BAI03.05	1. Verify that information security requirements are built into the solution.	70%	**70%**
				2. Implement controls to ensure security is addressed during the solution build/development.	70%	

Función	Categoría	Subcategoría	Referencias informativas	COBIT 2019- Actividades	Autoevaluacion	Promedio
PROTEGER (PR)	**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 las entidades de la organización), procesos y procedimientos para gestionar la protección de los sistemas de información y los activos.	**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).	**COBIT 5** BAI10.01	1. Provide the information security-related configuration, settings and system hardening to ensure that the information security posture of a given system is based on a set of requirements or architectural designs.	60%	78%
			COBIT 5 BAI10.02	1. Include an information security configuration for configurable items such as servers/hardware, network devices and endpoint devices.	90%	
				2. Identify information security requirements for current assets and take into account the dependencies.	80%	
				3. Secure all I&T baselines.	90%	
				4. Monitor compliance with established and approved secure configuration baselines and updates.	70%	
		PR.IP-2: Se implementa un ciclo de vida de desarrollo del sistema para gestionar los sistemas.	**COBIT 5** BAI03.03	1. Ensure solution components are properly secured.	40%	48%
			COBIT 5 BAI03.01	1. Define the information security specifications in line with high-level design.	40%	
				2. Create predefined sets of information security specifications along with suggested solutions for common cases.	40%	
			COBIT 5 BAI03.02	1. Integrate information security design into solution components.	70%	
		PR.IP-3: Se encuentran establecidos procesos de control de cambio de la configuración.	**COBIT 5** BAI06.01	1. Ensure that the information security policy adapts to business goals within an enterprise.	50%	30%
				2. Ensure that changes conform with the information security policy.	20%	
				3. Ensure that assessment of the potential impact of changes on information security is undertaken.	10%	
				4. Develop practices to consider the information security impact of emerging trends and technologies.	40%	
		PR.IP-4: Se realizan, se mantienen y se prueban copias de seguridad de la información.	**COBIT 5** DSS04.07	1. Ensure that information security requirements are included in the backup and restore arrangements.	80%	76%
			COBIT 5 DSS01.01	1. Verify that relevant information security operational procedures are included in the regular operational procedures.	80%	
				2. Ensure that the information processing life cycle (receipt, processing, storage and output) incorporates the information security policy and regulatory requirements.	70%	
				3. Ensure that information security operations are planned, performed, tested and controlled in line with the operational plan.	70%	
				4. Apply information security and access rights to all data.	80%	
		PR.IP-5: Se cumplen las regulaciones y la política con	**COBIT 5** DSS01.04	1. Ensure that environmental management adheres to information security	50%	50%
		PR.IP-6: Los datos son eliminados de acuerdo con las políticas.	**COBIT 5** BAI09.03	1. Identify and communicate the risk of information security noncompliance related to the asset life cycle.	30%	40%
				2. Ensure that information security measures and requirements are met throughout the asset life cycle.	70%	
				3. Identify end-of-life systems and plan for related information security risk	20%	
		PR.IP-7: Se mejoran los procesos de protección.	**COBIT 5** DSS04.05	1. Evaluate prior information security incidents to improve the BCP.	10%	10%
		PR.IP-8: Se comparte la efectividad de las tecnologías de protección.	**COBIT 5** BAI08.04	1. Securely dispose of information. Include deletion of traceability, especially in the case of personally identifiable information (PII), in conformance with relevant and applicable privacy laws and regulations	40%	40%
				2.Maintain and document a solid/accepted audit trail for information.	70%	
				3. Align information security measures relevant to classification.	20%	
				4. Develop secure information-destruction policies and processes	20%	
			COBIT 5 DSS03.04	1. Conduct root cause analysis, resolve information security problems and update the incident response plan.	50%	
		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)	**COBIT 5** APO12.06	1. Apply selected information security mitigation practices.	80%	50%
			COBIT 5 DSS04.03	1. Include information security requirements in the BCP and DRP.	20%	
		PR.IP-11: La seguridad cibernética se encuentra incluida en las prácticas de recursos humanos (por ejemplo, desaprovisionamiento, selección del personal).	**COBIT 5** APO07.01	1. Ensure that information security requirements are incorporated into the HR staffing and/or recruitment process for employees, contractors and vendors.	70%	46%
			COBIT 5 APO07.02	1. Ensure segregation of duties (SoD) in critical positions.	90%	
			COBIT 5 APO07.03	1. Obtain formal agreement from staff on information security policies and requirements.	10%	
				2. Provide professional development training and programs on information security.	40%	
				3. Use credentialing to augment a quality information security professional skill set.	60%	
				4. Establish appropriate enterprisewide education, training and awareness programs for information security.	40%	
			COBIT 5 APO07.04	1. Incorporate information security criteria in the personnel evaluation process.	10%	
		PR.IP-12: Se desarrolla y se implementa un plan de gestión de las vulnerabilidades.	**COBIT 5** BAI03.10	1. Verify that the solution is properly configured for inclusion in periodic information security reviews (e.g., vulnerability scan, patch monitoring, penetration test, controls testing, configuration review).	60%	70%
			COBIT 5 DSS05.01	1. Ensure that a vulnerability management program, including patch and configuration management, is in place.	90%	
				2. Ensure that antivirus, appropriate sandboxing and other advanced threat protection (ATP) measures are selected, deployed, monitored and maintained.	60%	
	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.	**COBIT 5** BAI03.10	1. Verify that the solution is properly configured for inclusion in periodic information security reviews (e.g., vulnerability scan, patch monitoring, penetration test, controls testing, configuration review).	60%	53%
			COBIT 5 BAI09.02	1. Define criticality levels and identify asset criticality in an asset register. 2	10%	
				2. Enforce information security requirements on assets.	80%	
				3. Include security measures (e.g., data center security reviews) that address third-party access to enterprise I&T facilities for onsite and off-site activities. Ensure appropriate security and privacy conditions, especially in the context of outsourcing.	100%	
				4. Ensure that the security classification of data is embedded in the asset inventory.	10%	
			COBIT 5 BAI09.03	1. Identify and communicate the risk of information security noncompliance related to the asset life cycle.	30%	
				2. Ensure that information security measures and requirements are met throughout the asset life cycle.	70%	
				3. Identify end-of-life systems and plan for related information security risk.	40%	
			COBIT 5 DSS01.05	1. Ensure that facilities management adheres to information security requirements.	80%	

Función	Categoría	Subcategoría	Referencias informativas	COBIT 2019- Actividades	Autoevaluacion	Promedio
PROTEGER (PR)	**Tecnología de protección (PR.PT):** Las soluciones técnicas de 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.	**PR.PT-1:** Los registros de auditoría o archivos se determinan, se documentan, se implementan y se revisan en conformidad con la política.	**COBIT 5** APO11.04	1. Define and monitor information security quality metrics and take corrective action where applicable.	50%	**42%**
			COBIT 5 BAI03.05	1. Verify that information security requirements are built into the solution.	70%	
				2. Implement controls to ensure security is addressed during the solution build/development.	70%	
			COBIT 5 MEA02.01	1. Perform a periodic review of information security and related policies and procedures.	20%	
				2. Determine the assurance scope (i.e., scope of information security controls to be assessed).	20%	
				3. Establish a formal approach to information security assurance.	20%	
		PR.PT-3: Se incorpora el principio de menor funcionalidad mediante la configuración de los sistemas para proporcionar solo las capacidades esenciales.	**COBIT 5** DSS06.06	1. Enforce data classification, acceptable use, and information security policies and procedures to support information asset protection.	70%	**70%**
		PR.PT-5: Se implementan mecanismos (por ejemplo, a prueba de fallas, equilibrio de carga, cambio en caliente o "hot swap") para lograr los requisitos de resiliencia en situaciones normales y adversas.	**COBIT 5** BAI04.01	1. Identify the technical and procedural information security issues related to availability, performance and capacity.	20%	**53%**
			COBIT 5 BAI04.02	1. Assess the information security impact of potential unavailability, underperformance and lack of capacity. 4	70%	
				2. Assess the business impact of potential unavailability, underperformance and lack of capacity due to introduction of information security controls.	70%	
				3. Assess the business impact of potential unavailability, underperformance and lack of capacity due to a potential information security incident.	70%	
			COBIT 5 BAI04.03	1. Assess the impact of new or changed service requirements on information security.	50%	
			COBIT 5 BAI04.05	1. Assess and investigate any information security issue that impacts availability, performance and capacity.	10%	
			COBIT 5 DSS01.05	1. Ensure that facilities management adheres to information security requirements.	80%	

Función	Categoría	Subcategoría	Referencias informativas	COBIT 2019- Actividades	Autoevaluacion	Promedio
DETECTAR (DE)	**Anomalías y Eventos (DE.AE):** se detecta actividad anómala	**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.	**COBIT 5** DSS03.01	1. Classify, categorize and prioritize information security problems.	70%	**70%**
		DE.AE-3: Cos datos de los eventos se recopilan y se correlacionan de múltiples fuentes y sensores.	**COBIT 5** BAI08.02	1. Map roles to knowledge areas and ensure that proper access control is in place for relevant information.	90%	**90%**
		DE.AE-4: Se determina el impacto de los eventos.	**COBIT 5** APO12.06	1. Apply selected information security mitigation practices.	80%	**75%**
			COBIT 5 DSS03.01	1. Classify, categorize and prioritize information security problems.	70%	
		DE.AE-5: Se establecen umbrales de alerta de incidentes.	**COBIT 5** APO12.06	1. Apply selected information security mitigation practices.	80%	**75%**
			COBIT 5 DSS03.01	1. Classify, categorize and prioritize information security problems.	70%	
	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	1. Actively monitor information security aspects of I&T infrastructure, including configuration, operations, access and use.	60%	**60%**
		DE.CM-2: Se monitorea el entorno físico para detectar posibles eventos de seguridad cibernética.	**COBIT 5** DSS01.04	1. Ensure that environmental management adheres to information security requirements.	50%	**65%**
			COBIT 5 DSS01.05	1. Ensure that facilities management adheres to information security requirements.	80%	
		DE.CM-4: Se detecta el código malicioso.	**COBIT 5** DSS05.01	1. Ensure that a vulnerability management program, including patch and configuration management, is in place.	90%	**75%**
				2. Ensure that antivirus, appropriate sandboxing and other advanced threat protection (ATP) measures are selected, deployed, monitored and maintained.	60%	
		DE.CM-5: Se detecta el código móvil no autorizado.	**COBIT 5** DSS05.01	1. Ensure that a vulnerability management program, including patch and configuration management, is in place.	90%	**75%**
				2. Ensure that antivirus, appropriate sandboxing and other advanced threat protection (ATP) measures are selected, deployed, monitored and maintained.	60%	
		DE.CM-6: Se monitorea la actividad de los proveedores de servicios externos para detectar posibles eventos de seguridad cibernética.	**COBIT 5** APO07.06	1. Obtain formal agreement from contract staff on information security policies and requirements.	50%	**37%**
				2. Establish formal policies and procedures for contract staff.	50%	
			COBIT 5 APO10.05	1. Review vendor information security performance.	10%	
		DE.CM-8: Se realizan escaneos de vulnerabilidades.	**COBIT 5** BAI03.10	1. Verify that the solution is properly configured for inclusion in periodic information security reviews (e.g., vulnerability scan, patch monitoring, penetration test, controls testing, configuration review).	60%	70%
			COBIT 5 DSS05.01	1. Ensure that a vulnerability management program, including patch and configuration management, is in place.	90%	
				2. Ensure that antivirus, appropriate sandboxing and other advanced threat protection (ATP) measures are selected, deployed, monitored and maintained.	60%	
	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.	**COBIT 5** APO01.02	1. Define the expectations with regard to information security, including specific organizational ethics and culture.	80%	**70%**
				2. Develop an information security awareness program.	50%	
				3. Establish metrics to measure behaviors regarding information security.	60%	
			COBIT 5 DSS05.01	1. Ensure that a vulnerability management program, including patch and configuration management, is in place.	90%	
				2. Ensure that antivirus, appropriate sandboxing and other advanced threat protection (ATP) measures are selected, deployed, monitored and maintained.	60%	
			COBIT 5 DSS06.03	1. Allocate access rights on the basis of need-to-know and least-privilege principles and job requirements.	70%	
				2. Periodically review authorizations.	80%	
		DE.DP-2: Las actividades de detección cumplen con todos los requisitos aplicables.	**COBIT 5** DSS06.01	1. Identify and prioritize IT and operational technology (OT) information security processes in line with business risk, compliance, etc.	60%	**67%**
				2. Identify and implement needed application controls.	60%	
			COBIT 5 MEA03.04	1. In the absence of third-party assurance, obtain evidence of compliance from third parties.	80%	
		DE.DP-4: Se comunica la información de la detección de eventos.	**COBIT 5** APO08.04	1. Establish appropriate communication channels between the information security function and the business.	100%	**73%**
				2. Establish appropriate reporting and metrics regarding information security.	70%	
			COBIT 5 APO12.06	1. Apply selected information security mitigation practices.	80%	
			COBIT 5 DSS02.05	1. Execute the information security incident response plan.	40%	
		DE.DP-5: los procesos de detección se mejoran continuamente.	**COBIT 5** DSS04.05	1. Evaluate prior information security incidents to improve the BCP.	50%	**50%**

Función	Categoría	Subcategoría	Referencias informativas	COBIT 2019- Actividades	Autoevaluacion	Promedio
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.	**COBIT 5** APO12.06	1. Apply selected information security mitigation practices.	80%	**80%**
	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.	**COBIT 5** APO12.03	1. Incorporate information security in the enterprise risk profile.	90%	**70%**
			COBIT 5 APO01.02	1. Define the expectations with regard to information security, including specific organizational ethics and culture.	80%	
				2. Develop an information security awareness program.	50%	
				3. Establish metrics to measure behaviors regarding information security.	60%	
		RS.CO-2: Los incidentes se informan de acuerdo con los criterios establecidos.	**COBIT 5** DSS01.03	1. Actively monitor information security aspects of I&T infrastructure, including configuration, operations, access and use.	90%	**90%**
		RS.CO-3: La información se comparte de acuerdo con los planes de respuesta.	**COBIT 5** DSS03.04	1. Conduct root cause analysis, resolve information security problems and update the incident response plan.	50%	**50%**
		RS.CO-4: La coordinación con las partes interesadas se realiza en consonancia con los planes de respuesta.	**COBIT 5** DSS03.04	1. Conduct root cause analysis, resolve information security problems and update the incident response plan.	50%	**50%**
		RS.CO-5: El intercambio voluntario de información se produce con las partes interesadas externas para lograr una mayor conciencia situacional de seguridad cibernética.	**COBIT 5** BAI08.04	1. Securely dispose of information. Include deletion of traceability, especially in the case of personally identifiable information (PII), in conformance with relevant and applicable privacy laws and regulations	40%	**38%**
				2.Maintain and document a solid/accepted audit trail for information.	70%	
				3. Align information security measures relevant to classification.	20%	
				4. Develop secure information-destruction policies and processes	20%	
	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.	**COBIT 5** DSS02.04	1. Maintain a procedure for evidence collection in line with applicable forensic evidence rules and regulations.	40%	**50%**
			COBIT 5 DSS02.07	1. Ensure that information security incidents and appropriate follow-up actions, including root cause analysis, adhere to existing incident and problem management processes.	60%	
				2. Drive resolution of investigations for information security-related incidents.	50%	
		RS.AN-2: Se comprende el impacto del incidente.	**COBIT 5** DSS02.02	1. Maintain an information security incident investigation and response procedure.	30%	**30%**
				2. Ensure that measures are in place to protect the confidentiality of information related to information security incidents.	30%	
				3. Implement a process to allow users to request information security guidance.	50%	
		RS.AN-3: Se realizan análisis forenses.	**COBIT 5** APO12.06	1. Apply selected information security mitigation practices.	80%	**65%**
			COBIT 5 DSS03.02	1. Investigate causes of and effects attributed to information security problems.	50%	
		RS.AN-4: Los incidentes se clasifican de acuerdo con los planes de respuesta.	**COBIT 5** DSS02.02	1. Maintain an information security incident investigation and response procedure.	30%	**37%**
				2. Ensure that measures are in place to protect the confidentiality of information related to information security incidents.	30%	
				3. Implement a process to allow users to request information security guidance.	50%	
	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.	**COBIT 5** APO12.06	1. Apply selected information security mitigation practices.	50%	**50%**
		RS.MI-2: Los incidentes son mitigados.	**COBIT 5** APO12.06	1. Apply selected information security mitigation practices.	50%	**50%**
		RS.MI-3: Las vulnerabilidades recientemente identificadas son mitigadas o se documentan como riesgos aceptados.	**COBIT 5** APO12.06	1. Apply selected information security mitigation practices.	50%	**50%**

Función	Categoría	Subcategoría	Referencias informativas	COBIT 2019- Actividades	Autoevaluacion	Promedio
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 seguridad cibernética.	**RC.RP-1:** El plan de recuperación se ejecuta durante o después de un incidente de seguridad cibernética.	**COBIT 5** APO12.06	1. Apply selected information security mitigation practices.	60%	**50%**
			COBIT 5 DSS02.05	1. Execute the information security incident response plan.	40%	
			COBIT 5 DSS03.04	1. Conduct root cause analysis, resolve information security problems and update the incident response plan.	50%	
	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.	**COBIT 5** APO12.06	1. Apply selected information security mitigation practices.	60%	**45%**
			COBIT 5 BAI05.07	1. Inform and train staff at periodic intervals based on information security needs.	30%	
		RC.IM-2: Se actualizan las estrategias de recuperación.	**COBIT 5** APO12.06	1. Apply selected information security mitigation practices.	60%	**50%**
			COBIT 5 BAI07.08	1.Ensure that information security is included in a post-implementation review.	40%	
	Comunicaciones (RC.CO): Las actividades de restauración se coordinan con partes internas y externas (por ejemplo, centros de coordinación, proveedores de servicios de Internet, propietarios de sistemas de ataque, víctimas, otros CSIRT y vendedores).	**RC.CO-3:** Las actividades de recuperación se comunican a las partes interesadas internas y externas, así como también a los equipos ejecutivos y de administración.	**COBIT 5** APO12.06	1. Apply selected information security mitigation practices.	60%	**60%**

Anexo 2

Programa de Actividades del Sistema de Gestión de Seguridad de la Información

Cod.	Actividad	Área	Frecuencia	Responsable	Tiempo	Año 2022
						Enero 1 2 3 4 | Febrero 1 2 3 4 | Marzo 1 2 3 4 | Abril 1 2 3 4 | Mayo 1 2 3 4 | Junio 1 2 3 4 | Julio 1 2 3 4 | Agosto 1 2 3 4 | Septiembre 1 2 3 4 | Octubre 1 2 3 4 | Noviembre 1 2 3 4 | Diciembre 1 2 3 4
DI-ID-01	Establecer proceso de evaluación de los riesgos de seguridad de la información, para identificar los riesgos asociados a la pérdida de la confidencialidad, integridad y disponibilidad de la información.	Todas las áreas	Anual	Ciso	12M	
DI-ID-02	Realizar el levantamiento y clasificación de los activos de información críticos según el tipo de información.	Todas las áreas	Anual	Ciso	12M	
DI-ID-03	Definir métricas que permitan medir el cumplimiento de la normativa interna respecto de seguridad de la información.	Todas las áreas	Anual	Ciso	4M	
DI-ID-04	Definir, coordinar, aprobar objetivos y requisitos de seguridad de la información dentro de la arquitectura de la institución.	Tecnología - Seguridad de la Información	Anual	PMO-Ciso	3M	
DI-ID-05	Documentar los controles de seguridad de la información que mantiene la institución e implementar escenarios y actividades de resiliencia para respuesta de ataques internos.	Tecnología - Seguridad de la Información	Anual	Ciso	6M	
DI-ID-06	Analizar, evaluar y formalizar normativa para ciberseguridad en la institución.	Tecnología - Seguridad de la Información	Anual	PMO-Ciso	3M	
DI-ID-07	Analizar, evaluar y formalizar normativa para el gobierno de ciberseguridad en la institución educativa.	Tecnología - Seguridad de la Información	Anual	PMO-Ciso	3M	
DI-ID-08	Analizar, evaluar y formalizar normativa para la evaluación de riesgos de ciberseguridad en la institución educativa.	Tecnología - Seguridad de la Información	Anual	PMO-Ciso	3M	
DI-ID-09	Completar el levantamiento de todas las vulnerabilidades de los servidores y aplicativos core y no core de la institución educativa.	Tecnología - Seguridad de la Información	Anual	PMO-Ciso	4M	
DI-ID-10	Levantar y definir una política para la gestión de seguridades cibernéticas con los proveedores.	Seguridad de la Información	Anual	Ciso	3M	
DI-PR-01	Incluir en el política de seguridad de la información de la institución educativa los procedimientos de acceso físico a la información.	Seguridad de la Información	Anual	Ciso	2M	
DI-PR-02	Elaborar y formalizar un plan de capacitación y evaluaciones sobre temas de seguridad y ciberseguridad de la información en la institución educativa.	Seguridad de la Información	Anual	Ciso	2M	
DI-PR-03	Diseñar e implementar un proceso que asegure a la información que se encuentra en reposo.	Seguridad de la Información	Anual	Ciso	2M	
DI-PR-04	Implementar un procedimiento formal para gestionar la protección de los sistemas de información y los activos.	Seguridad de la Información	Anual	Ciso	3M	
DI-PR-05	Establecer un procedimiento formal para el análisis y revisión de los logs identificados en el alcance de la evaluación de los aplicativos core y no core.	Seguridad de la Información	Semestral	Ciso	3M	
DI-DE-01	Diseñar e implementar una política para la gestión de incidentes conforme a la criticidad y asignación de prioridades para su resolución.	Seguridad de la Información	Anual	Ciso	2M	
DI-DE-02	Diseñar e implementar un proceso para monitorear los eventos de ciberseguridad.	Tecnología - Seguridad de la Información	Anual	PMO-Ciso	4M	
DI-DE-03	Elaborar un proceso formal para difundir y comunicar los eventos e incidentes de ciberseguridad.	Marketing - Seguridad de la Información	Anual	Jefe de Marketing-Ciso	4M	
DI-RS-01	Elaborar un proceso para la atención a incidentes de ciberseguridad.	Tecnología - Seguridad de la Información	Anual	Ciso	3M	
DI-RC-01	Elaborar un procedimiento de recuperación para asegurar la restauración de los sistemas afectados por los incidentes de ciberseguridad que incluyan procedimientos de comunicación interna y externa.	Tecnología - Seguridad de la Información - Marketing	Anual	PMO-Jefe de Marketing-Ciso	4M	

						Año 2022																																													
Cod.	Actividad	Área	Frecuencia	Responsable	Tiempo	Enero				Febrero				Marzo				Abril				Mayo				Junio				Julio				Agosto				Septiembre				Octubre				Noviembre				Diciembre			
						1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
DC-PO-01	Actualizar la Política de Seguridad de la información.	Seguridad de la Información	Anual	Ciso	1M																																																
DC-PO-02	Política para la clasificación de activos de la información	Seguridad de la Información	Anual	Ciso	2M																																																
DC-PO-03	Política para el manejo de los activos de información.	Seguridad de la Información	Anual	Ciso	2M																																																
DC-PO-04	Política para asignación de Funciones y responsabilidades de seguridad de la información	Seguridad de la Información	Anual	Ciso	2M																																																
DC-PO-05	Política para la asignación de recursos del SGSI.	Seguridad de la Información	Anual	Ciso	2M																																																
DC-PO-06	Política para evaluación de los riesgos de seguridad de la información.	Seguridad de la Información	Anual	Ciso	2M																																																
DC-PO-07	Política para el tratamiento de los riesgos de seguridad de la Información	Seguridad de la Información	Anual	Ciso	2M																																																
DC-PO-08	Política para la Concientización del SGSI	Seguridad de la Información	Anual	Ciso	2M																																																
DC-PO-09	Política para la Comunicación del SGSI	Seguridad de la Información	Anual	Ciso	2M																																																
DC-PO-10	Política para documentación de la información del SGSI.	Seguridad de la Información	Anual	Ciso	2M																																																
DC-PO-11	Políticas para efectuar Auditoría interna al SGSI.	Seguridad de la Información	Anual	Ciso	2M																																																
DC-PO-12	Políticas para no conformidades del SGSI.	Seguridad de la Información	Anual	Ciso	2M																																																
DC-PO-13	Política para la mejora contínua del SGSI	Seguridad de la Información	Anual	Ciso	2M																																																

Cod.	Actividad	Área	Frecuencia	Responsable	Tiempo	Año 2022
						Enero 1 2 3 4 | Febrero 1 2 3 4 | Marzo 1 2 3 4 | Abril 1 2 3 4 | Mayo 1 2 3 4 | Junio 1 2 3 4 | Julio 1 2 3 4 | Agosto 1 2 3 4 | Septiembre 1 2 3 4 | Octubre 1 2 3 4 | Noviembre 1 2 3 4 | Diciembre 1 2 3 4
AI-CT-02	Coordinar con el área de Recursos Humanos y Legal para incluir en los contratos con los proveedores las adendas que contengan parámetros mínimos de seguridad de la información que deben implementar y seguir los proveedores.	RRHH-Legal-Seguridad de la Información-Contraloría	Anual	RRHH-Jefe del área Legal-Cis	6M	
AI-CT-03	Definir e implementar un plan y cronograma de capacitaciones al personal administrador de base de datos.	RRHH-Seguridad de la Información-Tecnología	Anual	r de RRHH-Ciso-Jefe de Tecn	1M	
AI-CT-04	Definir e implementar un procedimiento que norme la asignación de parámetros para monitorear los incidentes de seguridad en las bases de datos, en la cual se detalle el responsable, la periodicidad y soporte de la ejecución.	Tecnología - Seguridad de la Información	Anual	Jefe de tecnología	3M	
AI-CT-05	Definir e implementar un procedimiento que norme los controles para efectuar los cambio en las configuraciones de la base de datos, en la cual se detalle el responsable, la periodicidad y soporte de la ejecución.	Tecnología - Seguridad de la Información	Anual	Jefe de tecnología	3M	
AI-CT-06	Definir e implementar un procedimiento que norme los controles para monitorear los derechos de acceso de los administradores, en la cual se detalle el responsable, la periodicidad y soporte de la ejecución.	Seguridad de la Información	Anual	Ciso	2M	
AI-CT-07	Diseñar e implementar un procedimiento que permita realizar un control periódico de los accesos sensitivos a usuarios que tienen acceso a las aplicaciones, en la cual se detalle el responsable, la periodicidad y soporte de la ejecución.	Seguridad de la Información	Anual	Ciso	2M	
AI-CT-08	Elaborar un manual de usuario que detalle el correcto uso de la interfaz.	Tecnología	Anual	Jefe de tecnología	2M	
AI-CT-09	Elaborar un procedimiento que genere reportes de fallas en los registros de administradores y operadores, en la cual se detalle el responsable, la periodicidad y soporte de la ejecución.	Tecnología	Anual	Jefe de tecnología	2M	
AI-CT-10	Elaborar un procedimiento que supervise al personal externo o de limpieza que tienen acceso a información sensitiva, en la cual se detalle el responsable, la periodicidad y soporte de la ejecución.	Seguridad de la Información	Anual	Ciso	2M	
AI-CT-11	Elaborar un procedimiento que supervise los derechos de acceso sobre los usuarios activos con permisos sensitivos, en la cual se detalle el responsable, la periodicidad y soporte de la ejecución.	Seguridad de la Información	Anual	Ciso	2M	
AI-CT-12	Implementar controles de monitoreo y revisión de los roles de acceso que se mantienen a las bases de datos.	Seguridad de la Información	Anual	Ciso	2M	
AI-CT-13	Implementar herramientas automáticas de detección de transacciones sensitivas en las bases de datos.	Seguridad de la Información	Anual	Ciso	2M	
AI-CT-14	Implementar herramientas para el registro de pistas de auditoría (logs) en base de datos.	Seguridad de la Información	Anual	Ciso	2M	
AI-CT-15	Incluir dentro de la estructura de la seguridad de la información las funciones y personal responsable de su ejecución.	Seguridad de la Información	Anual	Ciso	2M	