FACULTAD DE POSGRADOS

DESARROLLO DEL PROGRAMA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE UNA INSTITUCIÓN FINANCIERA

AUTOR

Darwin Roberto Cortez Quintana

AÑO

2021

FACULTAD DE POSGRADOS

DESARROLLO DEL PROGRAMA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE UNA INSTITUCIÓN FINANCIERA

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

Darwin Roberto Cortez Quintana

2021

RESUMEN

El desarrollo del programa de gestión de la seguridad de la información para la institución busca minimizar y optimizar los riesgos que se presentan en términos de seguridad de la información y ciberseguridad.

Se lo realizará mediante un análisis de la situación actual y su relación con las amenazas y vulnerabilidades de los entornos interno y externo, utilizando metodologías y marcos de trabajo reconocidos internacionalmente; para proponer una solución sistémica que consiste en una planificación de proyectos y planes de acción que se interrelacionan para lograr el objetivo común, que es disponer de una estrategia de seguridad para la institución.

El programa se enfocará en los controles de seguridad informática y se analizarán los beneficios que obtendrá la institución con su implementación, en términos de optimizar el riesgo.

ABSTRACT

The development of the information security management program for the institution seeks to minimize and optimize the risks that arise in terms of information security and cybersecurity.

It will be carried out through an analysis of the current situation and its relationship with the threats and vulnerabilities of internal and external environments, using internationally recognized methodologies and frameworks; to propose a systemic solution that consists of a planning of projects and action plans that are interrelated to achieve the common objective, which is to have a security strategy for the institution.

The program will focus on computer security controls and will analyze the benefits that the institution will obtain with its implementation, in terms of optimizing risk.

ÍNDICE DEL CONTENIDO

1. INTRODUCCIÓN

La transformación digital y el desarrollo de nuevas tecnologías ha dado un giro completo a la forma de hacer negocios, al mismo tiempo ha incrementado los riesgos para las empresas que no se protegen adecuadamente y se encuentran expuestas a estas nuevas amenazas.

Para la institución es un tema muy importante desarrollar y fortalecer el sistema de gestión de seguridad de la información, de manera que permita evitar posibles accesos no autorizados, robos de identidad, secuestro de información, *hackers*, *phishing*, correo no deseado (*spam*) y *malware* entre otros, que pudieran ocasionar pérdidas financieras y acabar con la confianza de los clientes, dañar la imagen y reputación de la institución en el mercado.

La mayor parte de la información se encuentra almacenada, transportada y accedida en los diferentes sistemas de información y tecnología, pero estos sistemas en continua evolución podrían presentar riesgos y amenazas que requieren ser evaluados y controlados.

2. DESARROLLO DEL TEMA

2.1 OBJETIVOS

2.1.1 OBJETIVO GENERAL

El objetivo principal del programa del Sistema de Gestión de Seguridad de la Información (SGSI) es el de mejorar la seguridad de la institución, mediante la protección de los activos de información frente a amenazas y riesgos que puedan

poner en peligro la confidencialidad, integridad, disponibilidad y privacidad; dentro y fuera de la institución, ante los clientes y demás partes interesadas del negocio.

2.1.2 OBJETIVOS DE LAS FASES

- Establecer el estado actual de la institución respecto la seguridad de la información, utilizando y comparando con marcos de trabajo reconocidos internacionalmente.

- Identificar y clasificar los diferentes tipos de información para proteger de manera adecuada, con base en la importancia de la información en la institución.

- Obtener un inventario de activos de información, de manera que se puedan identificar y clasificar por su criticidad para definir las responsabilidades y mecanismos de protección apropiados.

- Realizar la evaluación de riesgos en un activo crítico, obteniendo el conocimiento de las amenazas y vulnerabilidades que podrían impactar en este activo y definir planes de mitigación de los riesgos residuales identificados.

- Identificar y documentar ciertos documentos clave para complementar la estructura y operación del SGSI de la institución, además incluir los proyectos y planes de acción identificados en las fases anteriores.

2.2 FASE DE DIAGNÓSTICO

La primera fase para construir o fortalecer el SGSI es la de obtener un diagnóstico o estado de la situación actual de la institución en seguridad de la información, de manera que se pueda establecer una primera aproximación hacia el alcance general de las actividades o esfuerzos a ejecutar.

2.2.1 METODOLOGÍA UTILIZADA

Para la fase de diagnóstico se utiliza el marco de trabajo de ciberseguridad NIST CSF (*National Institute of Standards and Technology - Cybersecurity Framework*), que ofrece una referencia importante para cualquier organización que busca mejorar su seguridad. El marco de trabajo específica que el negocio conduce las actividades de seguridad de una organización y que los riesgos de seguridad deberían ser parte de los procesos de gestión de riesgos de la organización.

El marco de trabajo está compuesto de 3 partes: núcleo del marco, niveles de implementación y perfiles del marco.

NÚCLEO DEL MARCO DE TRABAJO DEL NIST				
Funciones del marco de trabajo				
Identificar - ID	**Proteger - PR**	**Detectar - DE**	**Responder - RS**	**Recuperar - RC**
Categorías				
Gestión de activos	Gestión de identidad y control de acceso	Anomalías y eventos	Análisis	Comunicaciones
Entorno empresarial	Conciencia y capacitación	Vigilancia continua de seguridad	Comunicaciones	Mejoras
Gobernanza	Seguridad de datos	Procesos de detección	Mejoras	Planificación de recuperación
Evaluación de riesgos	Procesos y procedimientos de protección de la información		Mitigación	
Estrategia de gestión de riesgos	Mantenimiento		Planificación de respuesta	
Gestión del riesgo de la cadena de suministro	Tecnología protectora			

Figura 1: Núcleo del marco de trabajo NIST CSF

Dentro de las categorías del núcleo, el marco de trabajo contiene un conjunto de actividades de seguridad, resultados deseados y referencias aplicables; para las referencias aplicables se utilizará el marco de trabajo de ISACA - COBIT 2019 área de enfoque seguridad de la información.

COBIT 2019 área de enfoque seguridad de la información proporciona una orientación relacionada con la seguridad de la información y cómo aplicar COBIT a temas específicos de seguridad de la información dentro de una empresa.

Para la evaluación del estado actual del SGSI con el marco de trabajo NIST CSF se utilizan los siguientes niveles de capacidad de COBIT 2019 para la evaluación e identificación del estado actual, con base en la evaluación de las prácticas y actividades de COBIT 2019 área de enfoque seguridad de la información.

Tabla 1

Niveles de capacidad COBIT 2019

Nivel	**Capacidad**
0	Incompleto
1	Realizado
2	Gestionado
3	Establecido
4	Previsible
5	Optimizado

Los diferentes niveles corresponden a la categorización que realiza el marco de trabajo COBIT 2019 respecto a las capacidades, con la siguiente descripción:

> “Nivel 0: Falta de cualquier capacidad básica, estrategia incompleta para abordar el propósito de gobierno y gestión y la intención de todas las prácticas del proceso puede haberse definido o no.
>
> Nivel 1: El proceso logra más o menos su propósito a través de la aplicación de un conjunto de actividades incompleto que pueden caracterizarse como iniciales o intuitivas, no muy organizadas.
>
> Nivel 2: El proceso lograr su propósito a través de la aplicación de un conjunto de actividades básicas, pero completas, que pueden caracterizarse como realizadas.
>
> Nivel 3: El proceso logra su propósito de forma mucho más organizada usando activos para la organización. Los procesos están, por lo general, bien definidos.
>
> Nivel 4: El proceso lograr su propósito, está bien definido, y su rendimiento se mide (de forma cuantitativa).
>
> Nivel 5: El proceso lograr su propósito, está bien definido, su rendimiento se mide para mejorar el desempeño y se persigue la mejora continua.” (Marco de Referencia COBIT 2019: Objetivos de gobierno y gestión, p. 20)

Con base en lo indicado anteriormente se establece una plantilla de Excel (Metodología y Estado Actual) incluida en el Anexo 1, con las diferentes funciones, categorías y subcategorías del marco de trabajo NIST CSF e incluido las referencias aplicables del marco de trabajo COBIT 2019 área de enfoque seguridad de la información con su detalle de prácticas y actividades.

Para la evaluación se establece una calificación con los niveles de capacidad indicados en la tabla 1, para obtener el nivel de capacidad actual y adicionalmente se establece un nivel de nivel de capacidad objetivo que corresponde al siguiente nivel del obtenido, sin que este nivel sea menor que 3

para garantizar que cumpla el propósito de cada una de las categorías y subcategorías.

2.2.2 RESULTADOS Y ENTREGABLES

Una vez que se evaluaron las diferentes prácticas y actividades de COBIT 2019 con base en las categorías y subcategorías del marco de trabajo NIST CSF, se obtienen los siguientes resultados que corresponden al estado actual del SGSI de la institución.

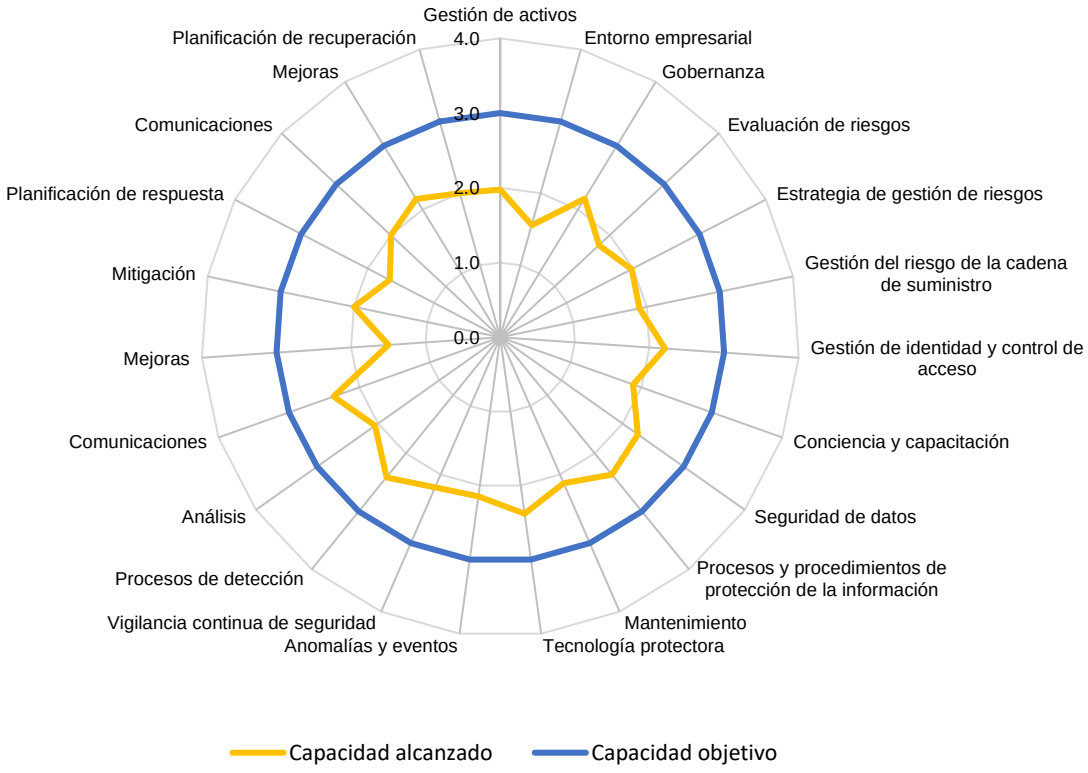


Figura 2: Estado actual del SGSI de la institución – subcategorías NIST CSF

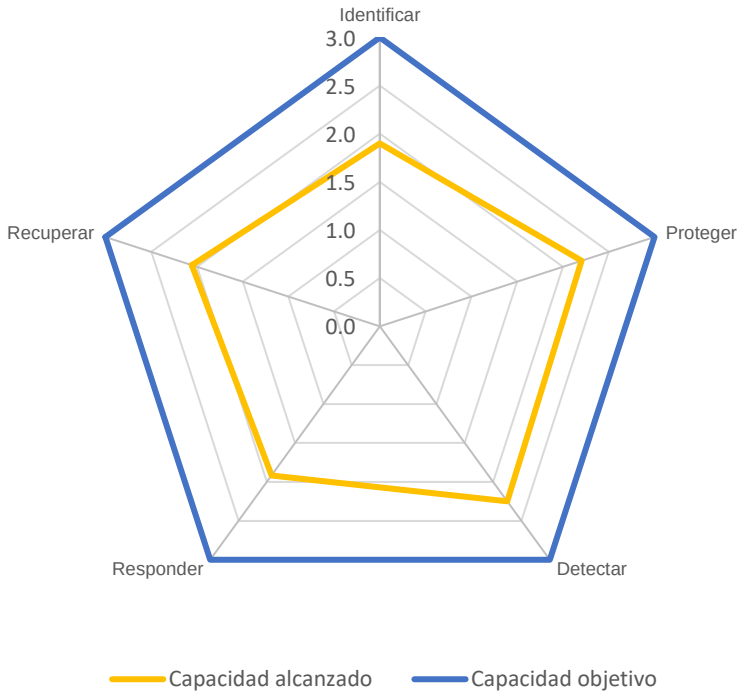


Figura 3: Estado actual del SGSI de la institución – categorías NIST CSF

Como entregable de la fase de diagnóstico se tiene la plantilla con la evaluación realizada e identificadas las oportunidades de mejora (Anexo 1), que se incluirán como proyectos y planes de mejora dentro del programa del SGSI.

2.2.3 CONCLUSIONES

- El estado actual del SGSI de la institución evaluado con base en el marco de trabajo NIST CSF, presenta un nivel de capacidad en general gestionado en el que se tienen algunas oportunidades de mejora. Si bien algunos puntos llegan al nivel de capacidad establecido, pero hay otros que en su conjunto reflejan el resultado general.

- Entre los puntos más importantes y para considerar su atención prioritaria se encuentran las funciones de Identificar y Responder en las cuales se

tiene una brecha mayor hacia el objetivo planteado, luego se encuentra la función de Recuperar y finalmente se debería fortalecer las funciones de Proteger y Detectar.

- Con relación a las subcategorías que se deben revisar de forma prioritaria son las mejoras dentro de la función Responder, con la incorporación de mejoras a los planes de respuesta aplicados previamente y que incluyan estrategias de respuesta.

- También con relación a las subcategorías se debe revisar principalmente lo referente al entorno empresarial dentro de la función Identificar, con la incorporación de mejoras a incluir dentro de las iniciativas de negocio a los temas de seguridad de la información; en general es importante se pueda incluir desde un inicio el análisis y alineación con temas de seguridad de la información.

2.3 FASE DE CLASIFICACIÓN DE LA INFORMACIÓN

La segunda fase para construir o fortalecer el SGSI es la de clasificar la información, para asegurar que reciba un nivel de protección adecuado de acuerdo con la importancia que tiene la información en la institución.

2.3.1 METODOLOGÍA UTILIZADA

Para la fase de clasificación de la información se realiza la definición de las entidades de información, es decir identificar personas, grupos de personas, productos, empresas u organismos que acceden, generan, almacenan o trasmiten los diferentes tipos de información en la institución.

Posteriormente y una vez identificadas las entidades de información se revisan en cada una de ellas los tipos de información que las entidades acceden, generan, almacenan o trasmiten.

Dentro de cada uno de los tipos de información se fueron incluyendo sus definiciones, de manera que se pueda identificar claramente a cada uno de los tipos de información.

Con la información descrita anteriormente se fue creando una plantilla en Excel (Tipos de Información e Identificación Activos) incluida en el Anexo 2.1, que contiene las entidades, tipos y definición del tipo de información.

Además de identificar los diferentes tipos de información es importante evaluar la calificación de impacto respecto a la seguridad de la información (confidencialidad, integridad, disponibilidad y privacidad) que tiene cada uno de los tipos de información; como se indicó al inicio de esta fase, servirá para asignar niveles de protección adecuados de acuerdo con la importancia que tiene la información.

Antes de evaluar el impacto en cada tipo de información, se realizó la definición del modulador de apetito de riesgo para la institución, considerando ciertos eventos de seguridad de la información.

A continuación, en la tabla 2 el modulador de apetito de riesgo considerado y en la tabla 3 los niveles de impacto del apetito de riesgo:

Tabla 2

Modulador de apetito de riesgo

Evento	Apetito de riesgo	Impacto del apetito de riesgo
Pérdidas financieras	Aversión	Mayor a 1 millón USD
Pérdidas reputación	Aversión	Pérdida de clientes mayor al 5%
Pérdida de la confidencialidad e integridad de la información	Agresivo	Número de incidentes de seguridad (confidencialidad e integridad)
Suspensión o pérdida total de los servicios electrónicos	Aversión	Número de incidentes de afectación del servicio
Fuga o robo de información de clientes	Neutral	Número incidentes con información crítica

Tabla 3

Niveles de impacto del apetito de riesgo

Niveles	Pérdidas financieras USD	Pérdidas de reputación	Pérdida de la confidencialidad e integridad de la información	Suspensión o pérdida total de los servicios electrónicos	Fuga o robo de información de clientes
CATASTROFICO	Desde 500K hasta 1 millón	Desde 1% hasta 5%	-	Servicios totalmente afectados	-
MAYOR	Desde 100K hasta 500K	Desde 0.1% hasta 1%	1 evento de seguridad mayor	Servicios parcialmente afectados	-
MODERADO	Hasta 100K	Hasta 0.1%	1 evento de seguridad moderado	Servicio intermitente	Incidente menor de robo o fuga de información (con pérdida de datos)
MENOR	-	-	2 eventos de seguridad menor	-	Incidente menor de robo o fuga de información (sin pérdida de datos)
INSIGNIFICANTE	-	-	3 eventos de seguridad leves	-	-

Se realizó la evaluación de los diferentes niveles de impacto respecto a los atributos de seguridad de la información, obteniendo niveles de impacto resultante para cada tipo de información.

Tabla 4

Niveles de impacto respecto a los atributos de seguridad de la información

Nivel	Impacto
1	Insignificante
2	Menor
3	Moderado
4	Mayor
5	Crítico

Para el cálculo del impacto resultante se evaluaron los atributos de confidencialidad, integridad y disponibilidad con el promedio de los 3 atributos y ponderándolos al 85%, sumado con el atributo de privacidad ponderado al 15%.

El campo resultado del impacto corresponde a la ponderación numérica del valor máximo y mínimo obtenidos en la columna total, dividido entre 5 que es la cantidad de niveles de impacto considerados. En la figura 4 se indica un ejemplo de los campos incluidos en la plantilla tipos de información.

Entidades	Tipos de Información	Definición del tipo de información	Impacto				Calificación Impacto					Resultado Impacto
			Confidencialidad	Integridad	Disponibilidad	Privacidad	C	I	D	P	Total	
PROSPECTOS	Información de contacto de prospectos	Incluye datos de nombre, dirección, teléfono, referencias	MODERADO	MODERADO	MODERADO	MAYOR	3	3	3	4	3.15	MODERADO

Figura 4: Campos incluidos en la plantilla de tipos de información

2.3.2 RESULTADOS Y ENTREGABLES

Se identificaron 8 entidades de información, entre los cuales están principalmente: clientes, empleados, proveedores y prospectos. Dentro de cada una de las entidades de información se definieron los tipos de información y su descripción.

Como entregable de la fase de clasificación de la información se tiene la plantilla (Anexo 2.1) con las entidades, tipos y definición de los tipos de información de la institución, además de la evaluación del impacto respecto a los diferentes atributos de seguridad de la información.

2.3.3 CONCLUSIONES

- Como resultado de la fase de clasificación de la información se identificaron y obtuvieron los diferentes tipos de información, con su respectivo impacto relacionado a los atributos de seguridad de la información.

- La información obtenida en esta fase resulta muy útil para la siguiente fase de identificación de activos, ya que se tiene los tipos de información críticos con base en la importancia de la información en la institución, para posteriormente considerar asegurarla de manera adecuada.

- Es muy importante determinar el apetito de riesgo de la institución respecto a los eventos de seguridad de la información, para poder evaluar de manera objetiva los impactos que se pudieran presentar respecto a la confidencialidad, integridad, disponibilidad y privacidad.

2.4 FASE DE INVENTARIO DE ACTIVOS DE INFORMACIÓN

La tercera fase para construir o fortalecer el SGSI es la de identificar los activos de información críticos para definir las responsabilidades y mecanismos de protección apropiados.

2.4.1 METODOLOGÍA UTILIZADA

Una vez que se clasificaron los diferentes tipos de información y determinó su impacto en la seguridad de la información, se puede ir analizando cada uno de los tipos de información cuyo impacto resultante en los atributos de seguridad de la información fueron críticos.

Se identifican los respectivos procesos, activos y componentes que acceden, generan, almacenan o trasmiten los diferentes tipos de información crítica en la institución. Se identifican 10 procesos que contienen tipos de información crítica y que incluyen diferentes entidades de información.

Dentro de los activos se identifican algunos sistemas de información y documentos que participan en los procesos identificados, se realiza la desagregación de los sistemas de información hacia los diferentes componentes de tecnología como servidores, bases de datos y otros componentes.

Finalmente se identifica el tipo de activo ya sea información digital o física y el propietario o responsable de la información, con el que se debería gestionar el ciclo de vida del activo.

Con la información descrita anteriormente se fue creando una plantilla en Excel (Tipos de Información e Identificación Activos) incluida en el Anexo 2.2, que

contiene los tipos de información, procesos, activos y componentes; además del tipo de activo y propietario o responsable.

2.4.2 RESULTADOS Y ENTREGABLES

Se identificaron 10 procesos que refieren a los tipos de información crítica y dentro de cada uno de los procesos se identificaron los activos y componentes que participan en cada proceso.

Como entregable de la fase de inventario de activos de información se tiene la plantilla (Anexo 2.2) con los tipos de información, procesos, activos y componentes identificados como críticos según la fase de clasificación de la información.

2.4.3 CONCLUSIONES

- Como resultado de la fase de inventario de activos de información se identificaron y obtuvieron los diferentes procesos, activos y componentes críticos con su respectivo propietario o responsable con el que se puede gestionar el ciclo de vida del activo.

- La información obtenida en esta fase resulta muy útil para la siguiente fase de análisis de riesgos de los activos, ya que se tiene activos críticos con base en la importancia de la información en la institución, para considerar protegerlos de manera adecuada.

- La metodología utilizada entre las fases 2 y 3 provee un mecanismo lógico para identificar los activos de información críticos, ya que en la práctica muchas veces se realiza primeo el inventario de activos y determina su

criticidad, pero no se ha analizado el origen y agrupación de la información y posteriormente los procesos, activos y componentes que intervienen en su tratamiento.

2.5 FASE DE EVALUACIÓN DE RIESGOS DE UN ACTIVO CRÍTICO

La cuarta fase para construir o fortalecer el SGSI es la de obtener un conocimiento de las amenazas y vulnerabilidades que podrían impactar a los activos de la institución, con base en el análisis de riesgos de los activos críticos. El alcance del programa de gestión del SGSI para el presente trabajo incluye la evaluación de riesgos de un activo tecnológico.

2.5.1 METODOLOGÍA UTILIZADA

Mediante la utilización de la taxonomía de MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) en su libro II – Catálogo de Elementos, se utilizan en esta fase los diferentes tipos de amenazas para los activos. El activo tecnológico crítico que se analiza es el servidor de base de datos, por lo que se revisan las diferentes amenazas que aplican a los componentes de hardware, software y comunicaciones de la base de datos.

Con los diferentes tipos de amenazas identificadas se revisan las vulnerabilidades que podrían ser explotadas para cada una de las amenazas, para lo cual se utiliza los puntos de referencia (CIS *Benchmarks*) desarrollados por el Centro para la Seguridad de Internet (*Center for Internet Security*) que provee un conjunto de mejores prácticas para ciberseguridad.

Se evalúan las diferentes recomendaciones respecto al tipo y versión de base de datos analizado, incluyendo en cada punto como vulnerabilidades si no se cumplieran con estas mejores prácticas.

Adicionalmente y para identificar vulnerabilidades en la parte de hardware y comunicaciones se utiliza la taxonomía de vulnerabilidades que incluye ISO 27005 para la gestión de riesgos.

Con la información de amenazas y vulnerabilidades referentes al activo analizado, se procede a evaluar el riesgo inherente para cada una de las vulnerabilidades, utilizando los niveles de probabilidad indicados en la tabla 6 y para la probabilidad se utiliza el modulador de apetito de riesgo, con los niveles de impacto de la tabla 4.

Tabla 6

Niveles de probabilidad

Nivel	Probabilidad	Porcentaje
1	Raro	2%
2	Poco Probable	5%
3	Posible	25%
4	Probable	75%
5	Casi Certeza	100%

Se identifica el riesgo inherente para cada una de las 76 posibles vulnerabilidades encontradas, ya que el riesgo inherente es intrínseco a cada activo y se calcula sin aplicar ningún control. Para determinar la severidad del riesgo se utiliza la siguiente matriz de calificación, como se indica en la figura 5.

MAPA DE CALIFICACIÓN SEVERIDAD DE RIESGO						
		IMPACTO				
		INSIGNIFICANTE	MENOR	MODERADO	MAYOR	CATASTRÓFICO
PROBABILIDAD	RARO	Bajo	Bajo	Moderado	Moderado	Alto
	POCO PROBABLE	Bajo	Bajo	Moderado	Alto	Alto
	POSIBLE	Bajo	Moderado	Moderado	Alto	Crítico
	PROBABLE	Bajo	Moderado	Alto	Crítico	Crítico
	CASI CERTEZA	Moderado	Moderado	Alto	Crítico	Crítico

Figura 5: Matriz de calificación de severidad de riesgo

Utilizando los mismos puntos de referencia (CIS *Benchmarks*) para el tipo y versión de base de datos analizado y controles de ISO 27002 como mejores prácticas, se definen los controles que serían requeridos para mitigar los diferentes riesgos; se evalúa también el control real aplicado en la institución, para posteriormente comparar los controles requeridos vs. aplicados.

Con base en la comparación anterior y dependiendo del tipo de control analizado, ya sea preventivo que comparado al control aplicado aportaría con un porcentaje de tratamiento a la probabilidad, detectivo o correctivo que comparado al control aplicado aportaría con un porcentaje de tratamiento al impacto, se calcula nuevamente la probabilidad e impacto luego de los controles aplicados por la institución, para finalmente obtener el riesgo residual de cada una de las vulnerabilidades y amenazas.

Para el cálculo de la probabilidad e impacto del riesgo residual se utiliza las siguientes fórmulas:

$$Probabilidad\ Final = Probabilidad\ Inicial * (1 - \%\ de\ Tratamiento\ Probabilidad) \quad (1)$$

$$Impacto\ Final = Impacto\ Inicial * (1 - \%\ de\ Tratamiento\ Impacto) \quad (2)$$

Con los valores anteriores de probabilidad e impacto final, se puede calcular el riesgo residual según la matriz de calificación de severidad de riesgo de la figura 5.

Durante la comparación de los controles requeridos y aplicados, se pudo ir identificando ciertos planes de acción que aplican a las vulnerabilidades y amenazas, estos planes de acción posteriormente serán identificados y priorizados para su recomendación.

Con la información descrita anteriormente se fue creando una plantilla en Excel (Riesgos) incluida en el Anexo 3, que contiene el análisis de amenazas, vulnerabilidades y controles, así como el cálculo del riesgo inherente y residual con base en la metodología descrita.

2.5.2 RESULTADOS Y ENTREGABLES

Luego de la evaluación de riesgos se tienen 76 riesgos identificados, de los cuales se tiene 1 riesgo residual alto, 9 riesgos residuales moderados y el resto son riesgos residuales bajos.

En la figura 6 se presentan de manera gráfica los resultados de riesgo residual alto y moderados para el activo crítico analizado.

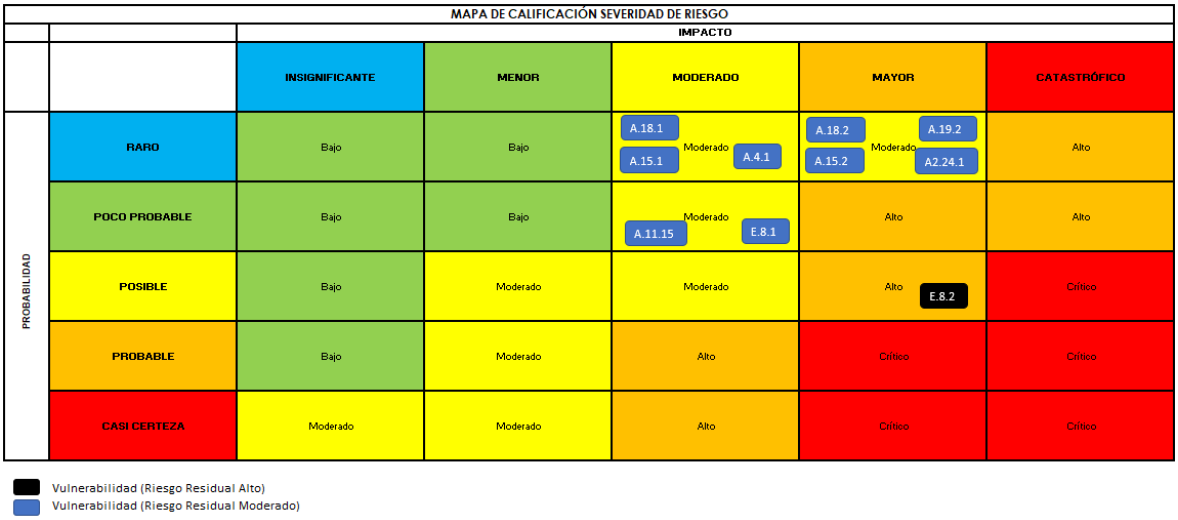


Figura 6: Resultados riesgo residual alto y moderados para el activo crítico analizado

Para el plan de acción se consideran tanto el riesgo residual alto, como los riesgos residuales moderados y bajos; en el caso de los riesgos residuales bajos no se considera en todos los casos algún plan de acción, sino más bien se aplican algunas mejoras.

Como entregable de la fase de evaluación de riesgos de un activo crítico se tiene la plantilla (Anexo 3) con el análisis de amenazas, vulnerabilidades y controles tanto requeridos como aplicados; además del cálculo del riesgo inherente, residual y planes de acción.

2.5.3 CONCLUSIONES

- Como resultado de la fase de evaluación de riesgo de un activo crítico se identificaron y obtuvieron las diferentes amenazas y vulnerabilidades para el activo analizado que en este caso es la base de datos; es muy importante contar con estos resultados y análisis para todos los activos

críticos, ya que permitirán aplicar diferentes planes de acción para mitigar los riesgos identificados.

- Con base en los resultados obtenidos se puede priorizar la aplicación de mejoras o inclusive nuevos controles para mitigar los riesgos identificados, ya que se tiene de una manera ordenada las amenazas, vulnerabilidades y riesgos.

- Se considera muy importante las fases anteriores del proyecto, ya que permitió identificar los activos críticos y con base en estos se evalúan los riesgos; sería poco práctico analizar todos los activos sin haberlos priorizado.

2.6 DOCUMENTOS CLAVE DEL SGSI

Luego de haber analizado los diferentes aspectos en cada una de las cuatro fases anteriores, es importante complementarlo con ciertos documentos que permitirán acotar la estructura y operación del programa del SGSI para la institución, además de incluir las oportunidades de mejora y planes de acción identificados en las fases anteriores.

2.6.1 DESARROLLO DE POLÍTICAS DE ALTO NIVEL

El objetivo de desarrollar políticas de alto nivel es el de proporcionar apoyo y orientación por parte de la dirección hacia los temas de seguridad de la información, buscando armonizar con los requisitos de negocio.

Las políticas deben ser comunicadas a todos los niveles, no solo de los responsables o directivos, sino también desde cada posición de la institución.

Se desarrolló un documento con las políticas de seguridad de la información de alto nivel, basado en los controles de ISO 27002 como marco de referencia. Se ajustaron u omitieron ciertos aspectos que no aplican a las características de la institución.

El Anexo 4 contiene el documento con las políticas de seguridad de alto nivel para la institución.

2.6.2 DEFINICIÓN DEL MODELO OPERACIONAL

El modelo operacional es la estructura de procesos como va a operar el SGSI, para lo cual se ha definido utilizar 5 macroprocesos principales y 23 procesos dentro de los macroprocesos.

La figura 7 presenta el modelo operacional del SGSI para la institución, que se encuentra basado en las funciones del marco de trabajo NIST CSF que fue utilizado en la fase de diagnóstico.

Figura 7: Modelo operacional del SGSI

Proceso Identificar: Dentro de las actividades y tareas interrelacionadas que incluyen este proceso se encuentran el comprender el contexto empresarial, identificar los recursos que respaldan las funciones críticas de la institución, riesgos de seguridad de la información, estrategia de gestión de riesgos y gobierno de seguridad de la información.

Proceso Proteger: Contiene actividades y tareas para desarrollar e implementar medidas de seguridad para limitar o contener el impacto de un evento de seguridad de la información, dentro de las cuales se encuentran la gestión de identidad y acceso, concientización y entrenamiento, protección de datos, mantenimiento y tecnologías de protección.

Proceso Detectar: Actividades y tareas interrelacionadas para identificar la ocurrencia de un evento de seguridad de la información, se incluye el descubrimiento oportuno de eventos de seguridad, monitoreo continuo de seguridad y detección.

Proceso Responder: Dentro de las actividades y tareas interrelacionadas que incluyen este proceso se encuentran la planificación de respuesta, comunicación, análisis, mitigación y mejoras para responder a un incidente de seguridad de la información detectado.

Proceso Recuperar: Incluye actividades y tareas para mantener planes de resiliencia y restablecer los servicios afectados por un incidente de seguridad de la información, considerando la planificación de recuperación, comunicaciones y mejoras.

Cada uno de los macroprocesos contienen un proceso interno de mejora continua, ya que de manera cíclica se ejecutan los 5 procesos para volver a evaluar y aplicar las mejoras hacia el objetivo del sistema de gestión de seguridad de la información.

2.6.3 MÉTRICAS DE LOS PROCESOS

En cada uno de los macroprocesos se definieron métricas para poder analizar el rendimiento hacia los objetivos de cada proceso del modelo operacional del SGSI.

Se encuentran definidas las siguientes métricas en cada macroproceso:

Identificar

- Porcentaje de proveedores críticos evaluados respecto a seguridad de la información.
- Tiempo promedio desde la última vez que se actualizaron los escenarios de riesgo.
- Porcentaje de activos con clasificación de seguridad definida en el inventario.

Proteger

- Número de incidentes (mayor o crítico) relacionados con acceso no autorizado a la información.
- Porcentaje de usuarios que completaron exitosamente los programas de concientización.

Detectar

- Porcentaje de falsos positivos descubiertos durante el monitoreo.
- Tiempo promedio para detectar los incidentes (menor, mayor o crítico) de seguridad.

Responder

- Porcentaje de incidentes de seguridad contenidos.
- Tiempo promedio para contener un incidente (mayor) luego de una alerta.

Recuperar

- Porcentaje de incidentes de seguridad resueltos.
- Tiempo promedio para determinar la solución de un incidente (mayor) luego de una alerta.

En la figura 8 se indican los macroprocesos y procesos con sus métricas.

Figura 8: Modelo operacional del SGSI y métricas

Para cada una de las métricas se definieron indicadores y metas con el objetivo por alcanzar de manera anual.

En la figura 9 se presentan las métricas anuales, indicadores y metas para cada macroproceso.

Macroproceso	Métrica anual	Indicador			Meta
Identificar	Porcentaje de proveedores críticos evaluados respecto a seguridad de la información	Alto	81%	100%	100%
		Medio	51%	80%	
		Bajo	0%	50%	
	Tiempo promedio desde la última vez que se actualizaron los escenarios de riesgo	Alto	4	Trimestral	Semestral
		Medio	2	Semestral	
		Bajo	1	Anual	
	Porcentaje de activos con clasificación de seguridad definida en el inventario	Alto	81%	100%	100%
		Medio	51%	80%	
		Bajo	0%	50%	
Proteger	Número de incidentes (mayor o crítico) relacionados con acceso no autorizado a la información	Alto	0		0 incidentes
		Medio	1		
		Bajo	2		
	Porcentaje de usuarios que completaron exitosamente los programas de concientización	Alto	81%	100%	100%
		Medio	51%	80%	
		Bajo	0%	50%	
Detectar	Porcentaje de falsos positivos descubiertos durante el monitoreo	Alto	15%	5%	10%
		Medio	60%	16%	
		Bajo	100%	61%	
	Tiempo promedio para detectar los incidentes (menor, mayor o crítico) de seguridad	Alto	60	30	60 minutos
		Medio	120	61	
		Bajo	240	121	
Responder	Porcentaje de incidentes de seguridad contenidos	Alto	81%	100%	100%
		Medio	51%	80%	
		Bajo	0%	50%	
	Tiempo promedio para contener un incidente (mayor) luego de una alerta	Alto	30	15	30 minutos
		Medio	60	31	
		Bajo	90	61	
Recuperar	Porcentaje de incidentes de seguridad resueltos	Alto	81%	100%	100%
		Medio	51%	80%	
		Bajo	0%	50%	
	Tiempo promedio para determinar la solución de un incidente (mayor) luego de una alerta	Alto	4	2	4 horas
		Medio	8	5	
		Bajo	24	9	

Figura 9: Métricas anuales, indicadores y metas para cada macroproceso

2.6.4 HOJA DE RUTA DE PLANES DE ACCIÓN

Con base en los resultados de las fases diagnóstico del estado actual del SGSI y evaluación de riesgos de un activo crítico, se identificaron oportunidades y planes de mejora.

Se realizó la priorización de las oportunidades de mejora en el caso del diagnóstico del estado actual del SGSI, considerando el margen de diferencia

entre la capacidad objetivo y la capacidad alcanzada de la evaluación en cada categoría del marco de trabajo NIST CSF.

Las oportunidades de mejora con diferencia entre la capacidad objetivo y alcanzada mayor a 1 se incluyeron como prioridad 1; las oportunidades de mejora con diferencia entre la capacidad objetivo y alcanzada iguales a 1 se incluyeron como prioridad 2 y el resto de las oportunidades de mejora con diferencia entre la capacidad objetivo y alcanzada menor que 1 se incluyeron con prioridad 3.

De la misma forma se realizó la priorización de los planes de mejora en el caso del análisis de riesgo, utilizando 3 prioridades; como primera prioridad los riesgos residuales moderados y alto, segunda prioridad los riesgos bajos por implementar y tercera prioridad los riesgos bajos por mejorar.

Con las tres prioridades de oportunidades y planes de mejora, se elaboró una hoja de ruta para el primer año, en la que los primeros 6 meses se utilizarán para cubrir las oportunidades y planes de mejora de prioridad 1; en los segundos 6 meses se cubrirán las oportunidades y planes de mejora de prioridad 2 y 3.

Las oportunidades y planes de mejora que corresponden al programa del SGSI se encuentran incluidas en el Anexo 5 (Hoja de Ruta Planes de Acción), la hoja de ruta resumida se presenta en la figura 10.

		Año 2022											
		Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
Activo: Base de Datos BD1 (Prioridad 1)													
PA	Plan de acción riesgos residual moderados y alto												
Estado actual SGSI (Prioridad 1)													
OM	Oportunidades de mejora del estado actual SGSI												
Activo: Base de Datos BD1 (Prioridad 2)													
PA	Plan de acción riesgos bajos por implementar												
Estado actual SGSI (Prioridad 2)													
OM	Oportunidades de mejora del estado actual SGSI												
Activo: Base de Datos BD1 (Prioridad 3)													
PA	Plan de acción riesgos bajos por mejorar												
Estado actual SGSI (Prioridad 3)													
OM	Oportunidades de mejora del estado actual SGSI												

Figura 10: Hoja de ruta de planes de acción

Tomando en cuenta que la evaluación de riesgos incluyó únicamente un activo crítico, se deberá ir incluyendo el resto de los activos críticos identificados o nuevos activos críticos mediante una evaluación continua de los activos y riesgos como proceso de mejora continua al SGSI.

3. CONCLUSIONES Y RECOMENDACIONES

- El desarrollo del presente trabajo de titulación, ha permitido revisar las diferentes fases para obtener el programa del sistema de gestión de seguridad de la información para una institución financiera, se ha partido desde la evaluación del estado actual del SGSI utilizando marcos de trabajo reconocidos internacionalmente, posterior se ha realizado la identificación de tipos de información y activos críticos, para luego evaluar el riesgo en torno a las amenazas y vulnerabilidades y finalmente definir una serie de planes,

proyectos e iniciativas que permitan lograr una estrategia de seguridad de la información para la institución.

- El programa del SGSI contiene una planificación de proyectos y planes de acción para proteger a la institución de los riesgos de seguridad de la información y ciberseguridad; sin embargo, este programa debe ser evaluado y actualizado regularmente, ya que pueden existir cambios en procesos, personas y tecnología que impliquen nuevos riesgos, además de presentarse nuevas amenazas internas y externas que podrían afectar a la seguridad de la institución.

- El alcance del presente trabajo de titulación incluyó la evaluación de un activo crítico tecnológico; sin embargo, como fueron identificados otros activos considerados críticos se debería como siguiente fase elaborar el análisis de riesgos, mediante la identificación de amenazas y vulnerabilidades que podrían impactar a estos activos. Se dispone de la metodología utilizada en el primer activo, por lo que facilitará la evaluación de este análisis; como resultado también se tendrán diferentes planes de mejora que se deben incluir en el programa del SGSI.

- Las instituciones financieras deben cumplir con ciertas normativas emitidas por el organismo de supervisión y control, en temas referentes a riesgos y seguridad de la información; durante la elaboración del programa del SGSI no se ha analizado esta normativa, sin embargo, al utilizar marcos de referencia reconocidos internacionalmente como COBIT 2019 y NIST CSF se están cumpliendo varios de estos puntos, pero se podría incluir dentro de la mejora continua al programa del SGSI se evalúe esta normativa posteriormente.
- Otro punto importante que se puede incluir dentro de la mejora continua respecto al programa del SGSI, es la evaluación del cumplimiento de la reciente aprobada Ley Orgánica de Protección de Datos Personales del Ecuador. Se recomienda utilizar como base el marco de trabajo NIST CSF

utilizado en el proyecto y mapear o emparejar los puntos relacionados a esta Ley, para posteriormente cubrir los puntos restantes si se encuentran dentro del SGSI. En general se ha utilizado como marco de referencia NIST CSF, sin embargo, el programa del SGSI no está limitado a este marco y se puede ir incluyendo los diferentes requerimientos personalizados para la institución.

4. REFERENCIAS

Center for Internet Security. (2016). *CIS Benchmark, v1.1.0.* Obtenido de CIS Benchmarks: https://www.cisecurity.org/cis-benchmarks/

GRC Software for Risk, Compliance, and Audit. (2021). *Calculating residual risk*. Obtenido de HighBond Help: https://help.highbond.com/helpdocs/highbond/en-us/Content/strategy/assessment/calculating_residual_risk.htm

Information Systems Audit and Control Association. (2018). *Marco de Referencia COBIT 2019: Objetivos de gobierno y gestión.* Schaumburg: ISACA.

Information Systems Audit and Control Association. (2020). *COBIT Focus Area: Information Security Using COBIT 2019.* Schaumburg: ISACA.

International Organization for Standardization; International Electrotechnical Commission;. (2013). *ISO/IEC 27002, Second edition, Information technology — Security techniques — Code of practice for information security controls.* Geneva: ISO/IEC.

International Organization for Standardization; International Electrotechnical Commission;. (2018). *ISO/IEC 27005:2018(en), Information technology — Security techniques — Information security risk management.* Geneva: ISO/IEC.

Ministerio de Hacienda y Administraciones Públicas, Gobierno de España. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid: Ministerio de Hacienda y Administraciones Públicas, Gobierno de España.

National Institute of Standards and Technology. (Abril de 2018). *Cybersecurity Framework Version 1.1.* Obtenido de Framework Documents | NIST: https://www.nist.gov/cyberframework/framework

Schreider, T., & Noakes-Fry, K. (2019). *Building an effective cybersecurity program, 2nd Edition.* Atlanta: Rosthstein Publishing.

ANEXOS

ANEXO 1:

PLANTILLA PARA EVALUACIÓN DEL ESTADO ACTUAL DEL SGSI

	A	B	C	D	E	F	G	H	L	M
1	Elemento del marco de referencia NIST	Descripción del elemento del marco de referencia NIST	Elemento del documento de referencia COBIT IS 2019	Prácticas del elemento del documento de referencia COBIT IS 2019	Actividades del elemento del documento de referencia COBIT IS 2019	Ref. Capacidad COBIT IS 2019	Calificación cuantitativa	Calificación resultante	Capacidad alcanzado	Capacidad objetivo
2	ID	Desarrolle una comprensión organizacional para administrar el riesgo de ciberseguridad para los sistemas, las personas, los activos, los datos y las capacidades.								
3	ID.AM	Los datos, el personal, los dispositivos, los sistemas y las instalaciones que permiten a la organización lograr los propósitos comerciales se identifican y administran de acuerdo con su importancia relativa para los objetivos organizacionales y la estrategia de riesgos de la								
4	ID.AM-1	Se realiza un inventario de los dispositivos y sistemas físicos dentro de la organización.	BAI09.01	BAI09.01 Identificar y registrar activos circulantes. Mantener un registro actualizado y preciso de todos los activos de I&T que se requieren para brindar servicios y que son propiedad o están controlados por la organización con una expectativa de beneficios futuros (incluidos los recursos con valor económico, como hardware o software). Garantice la alineación con la gestión de la configuración y la gestión financiera.	1. Visualice y documente los activos de I&T de la empresa para incluir el flujo de datos.	2				
5					2. Identificar los requisitos de seguridad de la información para los activos corrientes.	2				
6					3. Abordar la seguridad de la información para activos, datos y formularios de I&T, etc.	3				
7					4. Verificar que un inventario de activos completo y preciso informa la implementación de los procesos de seguridad (administración de parches, administración de vulnerabilidades, etc.).	3				
8			BAI09.02	BAI09.02 Gestionar activos críticos. Identifique los activos que son críticos para brindar capacidad de servicio. Maximice su confiabilidad y disponibilidad para respaldar las necesidades comerciales.	1. Defina los niveles de criticidad e identifique la criticidad de los activos en un registro de activos.	2				
9					2. Hacer cumplir los requisitos de seguridad de la información sobre los activos.	3				
10					3. Incluya medidas de seguridad (por ejemplo, revisiones de seguridad del centro de datos) que aborden el acceso de terceros a las instalaciones de I&T de la empresa para actividades dentro y fuera del sitio. Garantizar las condiciones adecuadas de seguridad y privacidad, especialmente en el contexto de la subcontratación.	3				
11					4. Asegúrese de que la clasificación de seguridad de los datos esté incorporada en el inventario de activos.	4				
12			BAI09.01	BAI09.01 Identificar y registrar activos circulantes. Mantener un registro actualizado y preciso de todos los activos de I&T que se requieren para brindar servicios y que son propiedad o están controlados por la organización con una expectativa de beneficios futuros (incluidos los recursos con valor económico, como hardware o software). Garantice la alineación con la gestión de la configuración y la gestión financiera.	1. Visualice y documente los activos de I&T de la empresa para incluir el flujo de datos.	2				
13					2. Identificar los requisitos de seguridad de la información para los activos corrientes.	2				
14					3. Abordar la seguridad de la información para activos, datos y formularios de I&T, etc.	3				
15					4. Verificar que un inventario de activos completo y preciso informa la implementación de los procesos de seguridad (administración de parches, administración de vulnerabilidades, etc.).	3				

	A	B	C	D	E	F	G	H	L	M
1	Elemento del marco de referencia NIST	Descripción del elemento del marco de referencia NIST	Elemento del documento de referencia COBIT IS 2019	Prácticas del elemento del documento de referencia COBIT IS 2019	Actividades del elemento del documento de referencia COBIT IS 2019	Ref. Capacidad COBIT IS 2019	Calificación cuantitativa	Calificación resultante	Capacidad alcanzado	Capacidad objetivo
431	PR	Desarrollar e implementar salvaguardas apropiadas para asegurar la entrega de servicios críticos.								
432	PR.AC	El acceso a los activos físicos y lógicos y las instalaciones asociadas se limita a los usuarios, procesos y dispositivos autorizados, y se gestiona de acuerdo con el riesgo evaluado de acceso no autorizado a las actividades y transacciones autorizadas.								
433	PR.AC-1	Las identidades y credenciales se emiten, administran, verifican, revocan y auditan para dispositivos, usuarios y procesos autorizados.	DSS05.04	DSS05.04 Gestionar la identidad del usuario y el acceso lógico. Asegúrese de que todos los usuarios tengan derechos de acceso a la información de acuerdo con los requisitos comerciales. Coordinar con las unidades de negocio que gestionan sus propios derechos de acceso dentro de los procesos de negocio.	1. Mantenga los derechos de acceso de los usuarios de acuerdo con la función comercial, los requisitos del proceso y las políticas de seguridad. Alinee la gestión de identidades y derechos de acceso a las funciones y responsabilidades definidas, en función de los principios de privilegio mínimo, necesidad de tener y necesidad de	2				
434					2. Administrar todos los cambios a los derechos de acceso (creación, modificaciones y eliminaciones) de manera oportuna basándose únicamente en transacciones aprobadas y documentadas autorizadas por las personas de la administración designadas.	3				
435					3. Separe, reduzca al mínimo necesario y administre activamente las cuentas de usuarios privilegiados. Asegúrese de monitorear toda la actividad en estas cuentas.	3				
436					4. Identifique de manera única todas las actividades de procesamiento de información por roles funcionales. Coordinar con las unidades de negocio para garantizar que todos los roles se definan de forma coherente, incluidos los definidos por la propia empresa dentro de las aplicaciones de procesos de negocio.	3				
437					5. Autenticar todo el acceso a los activos de información según el rol del individuo o las reglas comerciales. Coordinar con las unidades comerciales que administran la autenticación dentro de las aplicaciones utilizadas en los procesos comerciales para garantizar que los controles de autenticación se hayan administrado	3				
438					6. Asegúrese de que todos los usuarios (internos, externos y temporales) y su actividad en los sistemas de TI (aplicación comercial, infraestructura de TI, operaciones del sistema, desarrollo y mantenimiento) sean identificables de manera única.	3				
439					7. Mantener una pista de auditoría del acceso a la información en función de su sensibilidad y los requisitos reglamentarios.	4				
440					8. Realice una revisión de gestión periódica de todas las cuentas y los privilegios relacionados.	4				

	A	B	C	D	E	F	G	H	L	M
1	Elemento del marco de referencia NIST	Descripción del elemento del marco de referencia NIST	Elemento del documento de referencia COBIT IS 2019	Prácticas del elemento del documento de referencia COBIT IS 2019	Actividades del elemento del documento de referencia COBIT IS 2019	Ref. Capacidad COBIT IS 2019	Calificación cuantitativa	Calificación resultante	Capacidad alcanzado	Capacidad objetivo
940	DE	Desarrollar e implementar actividades apropiadas para identificar la ocurrencia de un evento de ciberseguridad.								
941	DE.AE	Se detecta actividad anómala y se comprende el impacto potencial de los eventos.								
942	DE.AE-1	Se establece y gestiona una línea de base de operaciones de red y flujos de datos esperados para usuarios y sistemas.	DSS03.01	DSS03.01 Identificar y clasificar problemas. Definir e implementar criterios y procedimientos para identificar y reportar problemas. Incluya la clasificación, categorización y priorización de problemas.	1. Clasificar, categorizar y priorizar los problemas de seguridad de la información.	2				
943	DE.AE-2	Los eventos detectados se analizan para comprender los objetivos y métodos de los ataques.	DSS05.07	DSS05.07 Gestione vulnerabilidades y supervise la infraestructura para detectar eventos relacionados con la seguridad. Utilizando una cartera de herramientas y tecnologías (por ejemplo, herramientas de detección de intrusos), gestione las vulnerabilidades y supervise la infraestructura en busca de acceso no autorizado. Asegúrese de que las herramientas de seguridad, las tecnologías y la detección estén integradas con la supervisión general de eventos y la gestión de incidentes.	1. Utilice continuamente una cartera de tecnologías, servicios y activos compatibles (por ejemplo, escáneres de vulnerabilidades, fuzzers y rastreadores, analizadores de protocolos) para identificar vulnerabilidades de seguridad de la información.	2				
944					2. Definir y comunicar los escenarios de riesgo, para que puedan reconocerse fácilmente y comprenderse la probabilidad y el impacto.	2				
945					3. Revise periódicamente los registros de eventos para detectar posibles incidentes.	2				
946					4. Asegúrese de que los tickets de incidentes relacionados con la seguridad se creen de manera oportuna cuando el monitoreo identifica posibles incidentes.	2				
947					5. Registre los eventos relacionados con la seguridad y conserve los registros durante el período apropiado.	3				
948			BAI08.01	BAI08.01 Identificar y clasificar fuentes de información para el gobierno y la gestión de I&T. Identifique, valide y clasifique diversas fuentes de información interna y externa necesarias para permitir la gobernanza y la gestión de I&T, incluidos documentos de estrategia, informes de incidentes e información de configuración que progresa desde el desarrollo hasta las operaciones antes de su puesta en funcionamiento.	1. Identificar los posibles usuarios del conocimiento, incluidos los propietarios de la información que puedan necesitar contribuir y aprobar el conocimiento. Obtenga los requisitos de conocimiento y las fuentes de información de los usuarios identificados.	2				
949					2. Considere los tipos de contenido (procedimientos, procesos, estructuras, conceptos, políticas, reglas, hechos, clasificaciones), artefactos (documentos, registros, video, voz) e información estructurada y no estructurada (expertos, redes sociales, correo electrónico, correo de voz, Fuentes de resumen de RichSite (RSS)).	2				
950					3. Clasifique las fuentes de información con base en un esquema de clasificación de contenido (por ejemplo, modelo de arquitectura de información). Asigne fuentes de información al esquema de clasificación.	3				
951					4. Recopilar, cotejar y validar las fuentes de información con base en los criterios de validación de la información (por ejemplo, comprensibilidad, relevancia, importancia, integridad, precisión, consistencia, confidencialidad, vigencia y confiabilidad).	4				

	A	B	C	D	E	F	G	H	L	M
1	Elemento del marco de referencia NIST	Descripción del elemento del marco de referencia NIST	Elemento del documento de referencia COBIT IS 2019	Prácticas del elemento del documento de referencia COBIT IS 2019	Actividades del elemento del documento de referencia COBIT IS 2019	Ref. Capacidad COBIT IS 2019	Calificación cuantitativa	Calificación resultante	Capacidad alcanzado	Capacidad objetivo
1093	RS	Desarrollar e implementar actividades apropiadas para tomar medidas con respecto a un incidente de ciberseguridad detectado.								
1094	RS.AN	El análisis se realiza para garantizar una respuesta eficaz y apoyar las actividades de recuperación.								
1095	RS.AN-1	Se investigan las notificaciones de los sistemas de detección	DSS02.04	DSS02.04 Investigar, diagnosticar y asignar incidencias. Identifique y registre los síntomas del incidente, determine las posibles causas y asigne para su resolución.	1. Mantener un procedimiento para la recolección de evidencia de acuerdo con las reglas y regulaciones de evidencia forense aplicables.	3				
1096			DSS02.07	DSS02.07 Realice un seguimiento del estado y genere informes. Realice un seguimiento, analice e informe periódicamente las incidencias y el cumplimiento de las solicitudes. Examine las tendencias para proporcionar información para la mejora continua.	1. Asegúrese de que los incidentes de seguridad de la información y las acciones de seguimiento adecuadas, incluido el análisis de la causa raíz, se adhieran a los procesos de gestión de incidentes y problemas existentes.	3				
1097					2. Impulsar la resolución de investigaciones de incidentes relacionados con la seguridad de la información.	4				
1098	RS.AN-2	Se entiende el impacto del incidente.	DSS02.02	DSS02.02 Registrar, clasificar y priorizar solicitudes e incidencias. Identifique, registre y clasifique las solicitudes de servicio e incidentes y asigne una prioridad de acuerdo con la importancia del negocio y los acuerdos de servicio.	1. Mantener un procedimiento de investigación y respuesta a incidentes de seguridad de la información.	2				
1099					2. Asegurarse de que existan medidas para proteger la confidencialidad de la información relacionada con incidentes de seguridad de la información.	2				
1100					3. Implementar un proceso que permita a los usuarios solicitar orientación sobre seguridad de la información.	3				
1101			DSS03.01	DSS03.01 Identificar y clasificar problemas. Definir e implementar criterios y procedimientos para identificar y reportar problemas. Incluya la clasificación, categorización y priorización de problemas.	1. Clasificar, categorizar y priorizar los problemas de seguridad de la información.	2				
1102			DSS03.02	DSS03.02 Investigar y diagnosticar problemas. Investigue y diagnostique problemas utilizando expertos en la materia relevantes para evaluar y analizar las causas raíz.	1. Investigar las causas y los efectos atribuidos a los problemas de seguridad de la información.	3				
1103			APO12.06	APO12.06 Responder al riesgo. Responder de manera oportuna a los eventos de riesgo materializados con medidas efectivas para limitar la magnitud de la pérdida.	1. Aplicar prácticas de mitigación de seguridad de la información seleccionadas.	3				
1104			APO12.06	APO12.06 Responder al riesgo. Responder de manera oportuna a los eventos de riesgo materializados con medidas efectivas para limitar la magnitud de la pérdida.	1. Aplicar prácticas de mitigación de seguridad de la información seleccionadas.	3				

	A	B	C	D	E	F	G	H	L	M
1	Elemento del marco de referencia NIST	Descripción del elemento del marco de referencia NIST	Elemento del documento de referencia COBIT IS 2019	Prácticas del elemento del documento de referencia COBIT IS 2019	Actividades del elemento del documento de referencia COBIT IS 2019	Ref. Capacidad COBIT IS 2019	Calificación cuantitativa	Calificación resultante	Capacidad alcanzado	Capacidad objetivo
1204	RC	Desarrollar e implementar actividades apropiadas para mantener planes de resiliencia y restaurar cualquier capacidad o servicio que se haya visto afectado debido a un incidente de ciberseguridad.								
1205	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 atacantes, víctimas, otros CSIRT y proveedores).								
1206	RC.CO-1	Se gestionan las relaciones públicas	EDM03.02	EDM03.02 Gestión de riesgo directo. Dirigir el establecimiento de prácticas de gestión de riesgos para proporcionar una seguridad razonable de que las prácticas de gestión de riesgos de I&T son apropiadas y que el riesgo de I&T real no excede el apetito de riesgo de la junta.	1. Dirigir la traducción e integración de la estrategia de riesgos de I&T en prácticas de gestión de riesgos y actividades operativas.	2				
1207					2. Dirigir el desarrollo de planes de comunicación de riesgos (que abarquen todos los niveles de la empresa).	2				
1208					3. Implementación directa de los mecanismos apropiados para responder rápidamente a los cambios de riesgo e informar inmediatamente a los niveles apropiados de gestión, respaldados por principios acordados de escalamiento (qué informar, cuándo, dónde y cómo).	2				
1209					4. Indique que el riesgo, las oportunidades, los problemas y las preocupaciones pueden ser identificados e informados por cualquier persona a la parte correspondiente en cualquier momento. El riesgo se debe gestionar de acuerdo con las políticas y procedimientos publicados y se debe escalar a los tomadores de decisiones relevantes.	2				
1210					5. Identificar los objetivos y métricas clave de los procesos de gestión y gobierno de riesgos a monitorear, y aprobar los enfoques, métodos, técnicas y procesos para capturar y reportar la información de medición.	3				
1211	RC.CO-2	La reputación se repara después de un incidente	MEA03.02	MEA03.02 Optimizar la respuesta a los requisitos externos. Revisar y ajustar políticas, principios, estándares, procedimientos y metodologías para asegurar que los requisitos legales, regulatorios y contractuales sean abordados y comunicados. Considere la posibilidad de adoptar y adaptar estándares de la industria, códigos de buenas	1. Revisar y ajustar periódicamente las políticas, los principios, los estándares, los procedimientos y las metodologías para que sean eficaces a la hora de garantizar el cumplimiento necesario y abordar el riesgo empresarial. Utilice expertos internos y externos, según sea necesario.	3				
1212					2. Comunicar los requisitos nuevos y modificados a todo el personal relevante.	3				
1213			APO12.06	APO12.06 Responder al riesgo. Responder de manera oportuna a los eventos de riesgo materializados con medidas efectivas para limitar la magnitud de la pérdida.	1. Aplicar prácticas de mitigación de seguridad de la información seleccionadas.	3				

Plantilla resumen evaluación y oportunidades de mejora:

	A	B	C	D	E	F	G	H
1	Identificador único de función	Función	Identificador único de categoría	Categoría	COBIT 2019 IS		Código Oportunidad de mejora	Oportunidad de mejora
2					Capacidad alcanzado	Capacidad objetivo		
3	ID	Identificar	ID.AM	Gestión de activos				
10			ID.BE	Entorno empresarial				
16			ID.GV	Gobernanza				
21			ID.RA	Evaluación de riesgos				
28			ID.RM	Estrategia de gestión de riesgos				
32			ID.SC	Gestión del riesgo de la cadena de suministro				
38	PR	Proteger	PR.AC	Gestión de identidad y control de acceso				
46			PR.AT	Conciencia y capacitación				
52			PR.DS	Seguridad de datos				
61			PR.IP	Procesos y procedimientos de protección de la información				
74			PR.MA	Mantenimiento				
77			PR.PT	Tecnología protectora				
83	DE	Detectar	DE.AE	Anomalías y eventos				
89			DE.CM	Vigilancia continua de seguridad				
98			DE.DP	Procesos de detección				
104	RS	Responder	RS.AN	Análisis				
110			RS.CO	Comunicaciones				
116			RS.IM	Mejoras				
119			RS.MI	Mitigación				
123			RS.RP	Planificación de respuesta				
125	RC	Recuperar	RC.CO	Comunicaciones				
129			RC.IM	Mejoras				
132			RC.RP	Planificación de recuperación				

ANEXO 2:

PLANTILLA PARA IDENTIFICACIÓN Y CLASIFICACIÓN DE LA INFORMACIÓN

Anexo 2.1: Plantilla tipos de Información

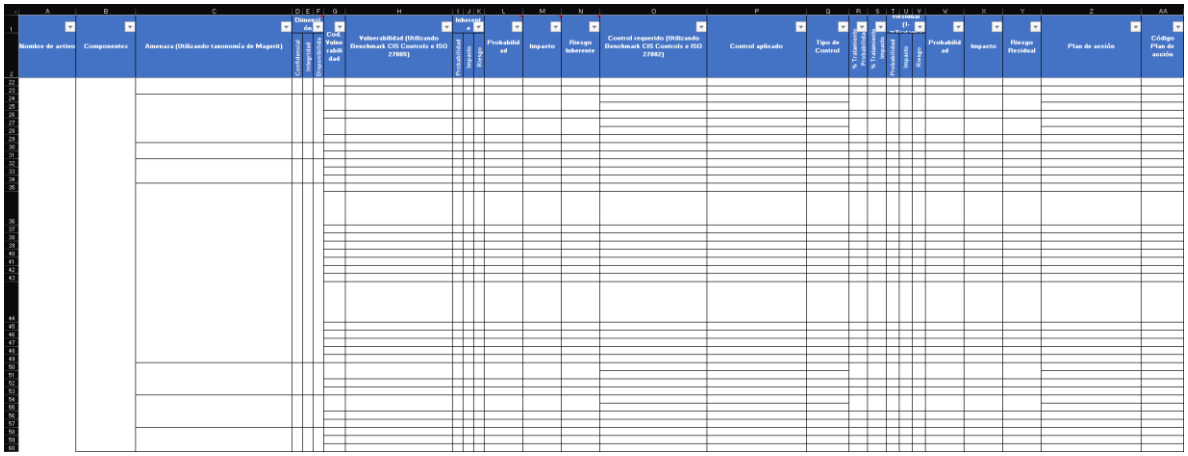
	A	B	C	D	E	F	G	H	I	J	K	L	M
1				Impacto				Calificación Impacto					
2	Entidades	Tipos de Información	Definición del tipo de información	Confidencialidad	Integridad	Disponibilidad	Privacidad	C	I	D	P	Total	Resultado Impacto
3													
4													
5													
6													
7													
8													
9													
10													
11													
12													
13													
14													
15													
16													
17													
18													
19													
20													
21													
22													
23													
24													
25													
26													
27													
28													

Anexo 2.2: Plantilla identificación de activos

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
1									Impacto				Calificación Impacto					
2	Entidades	Tipos de Información	Definición del tipo de información	Proceso	Activo	Componentes	Tipo de Activo	Propietario	Confidencialidad	Integridad	Disponibilidad	Privacidad	C	I	D	P	Total	Resultado Impacto
37																		
38																		
39																		
40																		
41																		
42																		
43																		
44																		
45																		
46																		
47																		
48																		
49																		
50																		
51																		
52																		
53																		
54																		
55																		
56																		
57																		
58																		
59																		
60																		

ANEXO 3:

PLANTILLA PARA EVALUACIÓN DE RIESGOS DE UN ACTIVO CRÍTICO



ANEXO 4:

POLÍTICAS DE SEGURIDAD DE ALTO NIVEL

1. Políticas internas de la institución:

1.1 Funciones y responsabilidades de la seguridad de la información

Definir y asignar las responsabilidades de seguridad de la información en la institución.

1.2 Separación de funciones

Implementar mecanismos para separar los deberes y áreas de responsabilidad en conflicto, para reducir las oportunidades de modificación o uso indebido no autorizado o involuntario de los activos de la institución.

1.3 Contacto con autoridades

Asegurar el adecuado contacto de la institución con las autoridades pertinentes (cumplimiento de la ley, organismos reguladores, autoridades de supervisión).

1.4 Contacto con grupos de interés especial

Asegurar el adecuado contacto de la institución con grupos de intereses especiales u otros foros especializados en seguridad y asociaciones profesionales.

1.5 Seguridad de la información en la gestión de proyectos

Implementar dentro de la gestión de proyectos el análisis de la seguridad de la información, independientemente del tipo de proyecto.

1.6 Política de dispositivos móviles

Implementar políticas y medidas de seguridad de apoyo para gestionar los riesgos introducidos por el uso de dispositivos móviles.

1.7 Teletrabajo

Implementar políticas y medidas de seguridad de apoyo para proteger la información a la que se accede, se procesa o se almacena en los sitios de teletrabajo.

2. Políticas de personal:

2.1 Selección

Implementar la verificación de antecedentes de todos los candidatos a un empleo en la institución y que se lleve a cabo de acuerdo con las leyes, reglamentos y ética pertinentes; también deben ser proporcionales a los requisitos comerciales, clasificación de la información a la que se debe acceder y los riesgos percibidos.

2.2 Términos y condiciones de empleo

Establecer acuerdos contractuales con empleados y contratistas que incluyan sus responsabilidades y las de la institución para la seguridad de la información.

2.3 Responsabilidades de la dirección

La gerencia debe exigir a todos los empleados y contratistas que apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos de la institución.

2.4 Concientización, educación y formación en seguridad de la información

Implementar mecanismos para impartir educación y capacitación adecuada de concientización en seguridad de la información, a todos los empleados de la institución y, cuando sea relevante, los contratistas; incluir actualizaciones periódicas de las políticas y procedimientos de la institución en seguridad de la información, según sea relevante para su función laboral.

2.5 Proceso disciplinario

Implementar un proceso disciplinario formal y comunicado para tomar medidas contra los empleados que hayan cometido una violación de la seguridad de la información.

2.6 Responsabilidades en la desvinculación

Definir, comunicar y hacer cumplir a los empleados o contratistas desvinculados las responsabilidades y deberes de seguridad de la información, que siguen siendo válidos después de la terminación o cambio de empleo.

3. Políticas de activos:

3.1 Inventario de activos

Implementar mecanismos para identificar los activos asociados con la información y las instalaciones de procesamiento de información, adicionalmente elaborar y mantener un inventario de estos activos.

3.2 Propiedad de los activos

Designar el propietario de los diferentes activos mantenidos en el inventario.

3.3 Uso aceptable de los activos

Implementar mecanismos para identificar y documentar reglas para el uso aceptable de la información y de los activos asociados con la información y las instalaciones de procesamiento de la información.

3.4 Devolución de activos

Implementar mecanismos para controlar la devolución por parte de los empleados y usuarios externos de todos los activos de la institución en su poder al terminar su empleo, contrato o acuerdo.

3.5 Clasificación de la información

Clasificar la información en términos de requisitos legales, valor, criticidad y sensibilidad a la divulgación o modificación no autorizadas.

3.6 Etiquetado de la información

Desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado de la información de acuerdo con el esquema de clasificación de la información adoptado por la institución.

3.7 Manejo de los activos

Desarrollar e implementar procedimientos para el manejo de activos de acuerdo con el esquema de clasificación de información adoptado por la institución.

3.8 Gestión de medios extraíbles

Implementar procedimientos para la gestión de medios removibles de acuerdo con el esquema de clasificación adoptado por la institución.

3.9 Eliminación de Soportes

Implementar procedimientos formales para desechar de forma segura cuando ya no se necesiten los medios.

3.10 Traslado de soportes físicos

Implementar mecanismos para proteger contra el acceso no autorizado, el mal uso o la corrupción de datos en los medios físicos que contienen información durante su transporte.

4. Políticas de control de acceso:

4.1 Política de control de acceso

Establecer, documentar y revisar una política de control de acceso en función de los requisitos comerciales y de seguridad de la información.

4.2 Acceso a las redes y a los servicios de red

Implementar mecanismos para controlar que los usuarios solo tengan acceso a la red y los servicios de red para los que hayan sido autorizados específicamente a utilizar.

4.3 Registro de usuarios y cancelación del registro

Implementar un proceso formal de registro y cancelación de registro de usuario para permitir la asignación de derechos de acceso.

4.4 Gestión de acceso a los usuarios

Implementar un proceso formal de aprovisionamiento de acceso de usuarios para asignar o revocar derechos de acceso para todos los tipos de usuarios a todos los sistemas y servicios de la institución.

4.5 Gestión de derechos de acceso privilegiados

Implementar mecanismos para restringir y controlar la asignación y uso de derechos de acceso privilegiado.

4.6 Gestión de la información de autenticación secreta de los usuarios

Implementar un proceso de gestión formal para controlar la asignación de información de autenticación secreta de los usuarios.

4.7 Revisión de derechos de acceso de usuario

Implementar los mecanismos para la revisión derechos de acceso de los usuarios a intervalos regulares por parte de los propietarios de los activos de información.

4.8 Remoción o ajuste de los derechos de acceso

Implementar mecanismos para eliminar los derechos de acceso de todos los empleados y usuarios externos que acceden a la información y las instalaciones de procesamiento de información al terminar su empleo, contrato o acuerdo, o ajuste en caso de modificaciones.

4.9 Uso de la información de autenticación secreta

Implementar mecanismos para asegurar que los usuarios sigan las prácticas de la institución en el uso de información secreta de autenticación.

4.10 Restricción de acceso a la información

Implementar mecanismos para restringir el acceso a la información y las funciones del sistema de aplicaciones de acuerdo con la política de control de acceso.

4.11 Procedimientos de conexión (inicio de sesión) seguros

Implementar mecanismos para controlar el acceso a los sistemas y aplicaciones mediante un procedimiento de inicio de sesión seguro, de acuerdo con la política de control de acceso.

4.12 Sistema de gestión de contraseñas

Implementar mecanismos para utilizar sistemas de gestión de contraseñas, los cuales deben ser interactivos y garantizar la calidad de las contraseñas.

4.13 Uso de programas utilitarios privilegiados

Implementar controles para restringir y controlar estrictamente el uso de programas de utilitarios que puedan ser capaces de anular los controles del sistema y de las aplicaciones.

4.14 Control de acceso al código fuente de programas

Implementar mecanismos para restringir el acceso al código fuente del programa.

5. Políticas de cifrado:

5.1 Política sobre el empleo de controles criptográficos

Desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.

5.2 Gestión de claves

Desarrollar e implementar una política sobre el uso, protección y vida útil de las claves criptográficas durante todo su ciclo de vida.

6. Políticas de seguridad física:

6.1 Perímetro de seguridad física

Definir y utilizar perímetros de seguridad física para proteger áreas que contienen información sensible o crítica e instalaciones de procesamiento de información.

6.2 Controles de acceso físico

Implementar mecanismos de control de entrada apropiados para las áreas seguras de manera que se garantice el acceso solo a personal autorizado.

6.3 Seguridad de oficinas e instalaciones

Diseñar y aplicar seguridad física para oficinas, salas e instalaciones.

6.4 Protección contra amenazas externas y del ambiente

Diseñar y aplicar protección física en las instalaciones contra desastres naturales, ataques malintencionados o accidentes.

6.5 El trabajo en las áreas seguras

Diseñar y aplicar procedimientos para trabajar en áreas seguras.

6.6 Ubicación y protección del equipamiento

Ubicar y proteger el equipamiento para reducir los riesgos de amenazas y peligros ambientales, y las oportunidades de acceso no autorizado.

6.7 Elementos de soporte

Implementar mecanismos para proteger el equipamiento contra cortes de energía y otras interrupciones causadas por fallas en los servicios públicos de apoyo.

6.8 Seguridad en el cableado

Implementar mecanismos para proteger el cableado de energía y telecomunicaciones que transporta datos o servicios de información de apoyo contra intercepciones, interferencias o daños.

6.9 Mantenimiento del equipamiento

Implementar esquemas de correcto mantenimiento del equipamiento para asegurar su disponibilidad e integridad continuas.

6.10 Retiro de bienes

Implementar mecanismos para controlar el traslado de equipos, información o software fuera de las instalaciones y sin autorización previa.

6.11 Seguridad del equipamiento y de los activos fuera de las instalaciones

Implementar mecanismos de seguridad para los activos fuera de las instalaciones, teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la institución.

6.12 Seguridad en la reutilización o eliminación de equipos

Implementar mecanismos para controlar que todos los elementos de los equipos que contienen medios de almacenamiento sean verificados, para garantizar que los datos confidenciales y el software con licencia se haya eliminado o sobrescrito de forma segura antes de su eliminación o reutilización.

6.13 Equipamiento desatendido por el usuario

Implementar mecanismos para asegurar que los usuarios no dejen sus equipos desatendidos y tengan la protección adecuada mientras realizan otras actividades.

6.14 Política de escritorio y pantalla limpios

Implementar políticas de escritorio limpio para documentos físicos y medios de almacenamiento extraíbles, además de políticas de pantalla limpia para las instalaciones de procesamiento de información.

7. Políticas de seguridad operacional:

7.1 Procedimientos documentados de operación

Documentar y poner a disposición de todos los usuarios que lo requieran, los diferentes procedimientos operativos.

7.2 Gestión de cambios

Implementar mecanismos para controlar los cambios, procesos comerciales, instalaciones y los sistemas de procesamiento de información de la institución que afectan la seguridad de la información.

7.3 Gestión de la capacidad

Implementar mecanismos para monitorear, ajustar y hacer proyecciones de los requisitos de capacidad futuros, respecto al uso de los recursos para asegurar el desempeño requerido del sistema.

7.4 Separación de los ambientes de desarrollo, prueba y operación

Implementar mecanismos para asegurar la separación de entornos de desarrollo, pruebas y producción para reducir los riesgos de acceso no autorizado o cambios en el entorno operativo de producción.

7.5 Controles ante software malicioso

Implementar controles de detección, prevención y recuperación para proteger contra malware a los equipos, adicionalmente combinar con la concienciación adecuada del usuario.

7.6 Respaldo de la información

Implementar mecanismos para copias de información, software e imágenes del sistema, de manera que sean obtenidas y probadas regularmente de acuerdo con una política de copias de seguridad acordada.

7.7 Registro de eventos

Implementar mecanismos para generar, mantener y revisar periódicamente los registros de eventos de actividades de los usuarios, excepciones, fallas y eventos de seguridad de la información.

7.8 Protección de la información de registros (logs)

Implementar mecanismos para proteger contra manipulación y acceso no autorizado a la información de registro de eventos y equipos o ubicaciones que los contienen.

7.9 Registros del administrador y operador

Implementar mecanismos para proteger y revisar de manera periódica los registros de eventos de las actividades del administrador y del operador del sistema.

7.10 Sincronización de relojes

Implementar mecanismos para la sincronización con una única fuente de tiempo de referencia a los relojes de todos los sistemas de procesamiento de información relevantes dentro la institución.

7.11 Instalación de software en los sistemas de producción

Implementar mecanismos o procedimientos para controlar la instalación y cambios de software, aplicaciones y programas en los sistemas de producción.

7.12 Gestión de vulnerabilidades técnicas

Implementar mecanismos para recibir, analizar y gestionar las vulnerabilidades técnicas; la información sobre vulnerabilidades técnicas de los sistemas de información que se utilizan debe obtenerse de manera oportuna, evaluarse la exposición de la institución a dichas vulnerabilidades y tomar las medidas adecuadas para abordar el riesgo asociado.

7.13 Restricciones en la instalación de software

Establecer e implementar reglas que rijan la instalación de software por parte de los usuarios, considerando el principio de mínimos privilegios.

7.14 Controles de auditoría de sistemas de información

Implementar mecanismos para acordar la revisión de requisitos de auditoría y actividades que implican la verificación de los sistemas en producción, las

revisiones deben planificarse y acordarse cuidadosamente para minimizar las interrupciones en los procesos comerciales.

8. Políticas de seguridad en las comunicaciones:

8.1 Controles de Red

Implementar mecanismos de administración y control de las redes para proteger la información en sistemas y aplicaciones.

8.2 Seguridad de los servicios de red

Identificar e incluir en acuerdos de servicio de red a todos los mecanismos de seguridad, niveles de servicio y requisitos de gestión, ya sea que estos servicios se proporcionen internamente o se subcontraten.

8.3 Separación en redes

Implementar mecanismos de separación en redes para los diferentes grupos de servicios de información, usuarios y sistemas de información.

8.4 Políticas y procedimientos de intercambio de información

Implementar políticas, procedimientos y controles formales de transferencia para proteger el intercambio de información mediante el uso de cualquier tipo de instalaciones de comunicación.

8.5 Acuerdos de intercambio de información

Desarrollar acuerdos de intercambio de información que aborden la transferencia segura de información comercial entre la institución y partes externas.

8.6 Mensajería electrónica

Implementar mecanismos para proteger adecuadamente la información involucrada en la mensajería electrónica.

8.7 Acuerdos de confidencialidad y de no divulgación

Identificar, revisar y documentar periódicamente los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la institución para la protección de la información.

9. Políticas de ciclo de vida del desarrollo de sistemas:

9.1 Análisis y especificación de los requisitos de seguridad

Incluir los requisitos relacionados con la seguridad de la información dentro del levantamiento de información y requerimientos para los nuevos sistemas de información o las mejoras a los sistemas de información existentes.

9.2 Aseguramiento de los servicios de aplicación en las redes públicas

Implementar mecanismos para asegurar los servicios de aplicación en redes públicas, considerar que la información involucrada en los servicios de aplicaciones que pasan por redes públicas debe protegerse de actividades fraudulentas, disputas contractuales y divulgación o modificación no autorizadas.

9.3 Transacciones en línea

Implementar mecanismos para proteger la información involucrada en las transacciones de servicios de aplicaciones, de manera que se evite la transmisión incompleta, enrutamiento incorrecto, alteración no autorizada de mensajes, divulgación no autorizada y duplicación o reproducción no autorizada de mensajes.

9.4 Política de desarrollo seguro

Establecer y aplicar reglas a los desarrollos dentro de la institución, considerando a la seguridad de la información para el desarrollo de software y sistemas.

9.5 Procedimiento de control de cambio del sistema

Establecer procedimientos formales de control de cambios para controlar los cambios en los sistemas dentro del ciclo de vida del desarrollo.

9.6 Revisión técnica de aplicaciones después de cambios de las plataformas operativas

Establecer revisiones técnicas y pruebas de las aplicaciones críticas para el negocio cuando se cambian las plataformas operativas, para garantizar que no haya un impacto adverso en las operaciones o la seguridad de la institución.

9.7 Restricciones a los cambios en los paquetes de software

Implementar mecanismos para limitar las modificaciones a los paquetes de software, solo a los cambios necesarios, adicionalmente controlar estrictamente todos los cambios.

9.8 Principios de la ingeniería de Sistemas Seguros

Establecer, documentar, mantener y aplicar principios para la ingeniería de sistemas seguros en cualquier esfuerzo de implementación de sistemas de información.

9.9 Ambiente de desarrollo seguro

Establecer entornos de desarrollo seguro para el desarrollo de los sistemas y esfuerzos de integración que cubren todo el ciclo de vida del desarrollo del sistema.

9.10 Desarrollo subcontratado

Implementar mecanismos para supervisar y monitorear la actividad de desarrollo de sistemas subcontratados.

9.11 Pruebas de seguridad del sistema

Establecer pruebas de la funcionalidad de seguridad durante el desarrollo.

9.12 Pruebas de aceptación del sistema

Establecer programas de prueba de aceptación y criterios relacionados para nuevos sistemas de información, actualizaciones y nuevas versiones.

9.13 Protección de datos de prueba

Implementar mecanismos para seleccionar adecuadamente, proteger y controlar los datos de prueba.

10. Políticas de proveedores y terceros:

10.1 Política de seguridad de la información para las relaciones con los proveedores

Acordar y documentar con el proveedor los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso del proveedor a los activos de la institución.

10.2 Tener en cuenta la seguridad en los acuerdos con proveedores

Establecer y acordar requisitos de seguridad de la información relevantes con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de TI para la seguridad de la información de la institución.

10.3 Cadena de suministro de tecnologías de la información y las comunicaciones

Establecer controles para asegurar que los acuerdos con los proveedores incluyan requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y las comunicaciones y la cadena de suministro de los productos.

10.4 Seguimiento y revisión de los servicios de proveedores

Establecer mecanismos para monitorear, revisar y auditar periódicamente la prestación de servicios de los proveedores.

10.5 Gestión de cambios en los servicios de los proveedores

Establecer mecanismos de gestión de cambios en la prestación de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas,

procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la importancia de la información, sistemas y procesos comerciales involucrados y la reevaluación de los riesgos.

11. Políticas de gestión de incidentes:

11.1 Responsabilidades y procedimientos

Establecer responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.

11.2 Reporte de eventos de seguridad de la información

Establecer mecanismos para reportar los eventos de seguridad de la información, los cuales deben notificarse a través de los canales de gestión adecuados lo antes posible.

11.3 Reporte de debilidades de seguridad de la información

Establecer mecanismos para exigir a los empleados y contratistas que utilicen los sistemas y servicios de información de la institución que registren y notifiquen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.

11.4 Evaluación y decisión sobre los eventos de seguridad de información

Establecer mecanismos de evaluación y clasificación de incidentes de seguridad, los eventos de seguridad de la información deben evaluarse determinar si clasifican como incidentes de seguridad de la información.

11.5 Respuesta a incidentes de seguridad de la información

Implementar mecanismos de respuesta a incidentes de seguridad de la información, los cuales deben responderse de acuerdo con los procedimientos documentados.

11.6 Aprendiendo de los incidentes de seguridad de la información

Establecer mecanismos para utilizar la información de incidentes de seguridad pasados como aprendizaje y conocimiento para afrontar nuevos incidentes, el conocimiento obtenido al analizar y resolver incidentes de seguridad de la información debe usarse para reducir la probabilidad o el impacto de incidentes futuros.

11.7 Recolección de evidencia

Establecer mecanismos para definir y aplicar procedimientos para la identificación, recopilación, adquisición y preservación de información que pueda servir como evidencia.

12. Políticas de gestión de la continuidad del negocio:

12.1 Planificación de la continuidad de la seguridad de la información

Establecer una planificación de la continuidad de la seguridad de la información mediante la determinación de requisitos de seguridad de la información y continuidad en situaciones adversas durante una crisis o un desastre.

12.2 Implementación de la continuidad de seguridad de la información

Establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel requerido de continuidad para la seguridad de la información durante una situación adversa.

12.3 Verificar, revisar y evaluar la continuidad de la seguridad de la información

Verificar los controles de continuidad de seguridad de la información establecidos e implementados a intervalos regulares para asegurar que sean válidos y efectivos durante situaciones adversas.

12.4 Disponibilidad de las instalaciones de procesamiento de información

Implementar instalaciones de procesamiento de información con suficiente redundancia para cumplir con los requisitos de disponibilidad.

13. Políticas de cumplimiento:

13.1 Identificación de la legislación aplicable y de los requisitos contractuales

Identificar, documentar y mantener actualizados los requisitos legales, reglamentarios y contractuales relevantes para cada sistema de información de la institución.

13.2 Protección de los registros

Establecer mecanismos para proteger los registros de cuentas, transacciones, bases de datos, registros de auditoría y procedimientos operacionales contra pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada, de acuerdo con los requisitos legales, reglamentarios, contractuales y comerciales.

13.3 Protección de los datos y privacidad de la información personal

Garantizar la privacidad y protección de la información de identificación personal según lo requiera la legislación y reglamentación pertinente.

13.4 Regulación de los controles criptográficos

Verificar y establecer el cumplimiento de controles criptográficos utilizados de conformidad con todos los acuerdos, legislación y reglamentaciones pertinentes.

13.5 Revisión independiente de la seguridad de la información

Establecer revisiones de forma independiente y a intervalos planificados sobre el enfoque de la institución para gestionar la seguridad de la información y su implementación (es decir, objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información). La revisión también debe realizarse cuando se produzcan cambios significativos.

13.6 Cumplimiento de la política y las normas de seguridad

Establecer responsabilidades en las diferentes áreas de la institución para la revisión periódica del cumplimiento de políticas y estándares de seguridad en los diferentes procesos y procedimientos dentro de su área de responsabilidad.

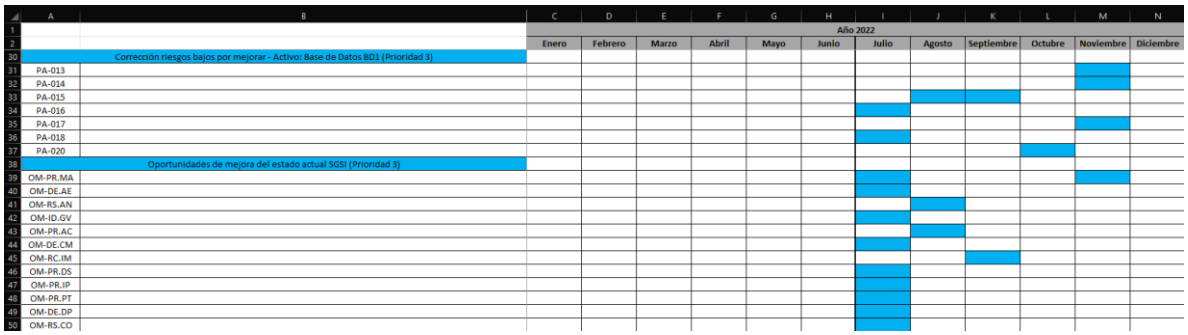
13.7 Revisión del cumplimiento técnico

Establecer mecanismos para verificar el cumplimiento de las políticas y estándares de seguridad de la información de la institución en los sistemas de información, la revisión debe realizarse de manera periódica.

ANEXO 5:

OPORTUNIDADES Y PLANES DE MEJORA DEL PROGRAMA DEL SGSI

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1			Año 2022											
2			Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
3	Corrección riesgos residual moderados y alto - Activo: Base de Datos BD1 (Prioridad 1)													
4	PA-001													
5	PA-003													
6	PA-004													
7	PA-005													
8	PA-007													
9	PA-011													
10	PA-012													
11	PA-019													
12	Oportunidades de mejora del estado actual SGSI (Prioridad 1)													
13	OM-RS.IM													
14	OM-ID.BE													
15	OM-RS.RP													
16	OM-ID.RA													
17	OM-ID.SC													
18	OM-PR.AT													
19	Corrección riesgos bajos por implementar - Activo: Base de Datos BD1 (Prioridad 2)													
20	PA-002													
21	PA-008													
22	PA-009													
23	PA-010													
24	Oportunidades de mejora del estado actual SGSI (Prioridad 2)													
25	OM-ID.AM													
26	OM-ID.RM													
27	OM-RS.MI													
28	OM-RC.CO													
29	OM-RC.RP													



	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1			Año 2022											
2			Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
30	Corrección riesgos bajos por mejorar - Activo: Base de Datos BD1 (Prioridad 3)													
31	PA-013													
32	PA-014													
33	PA-015													
34	PA-016													
35	PA-017													
36	PA-018													
37	PA-020													
38	Oportunidades de mejora del estado actual SGSI (Prioridad 3)													
39	OM-PR.MA													
40	OM-DE.AE													
41	OM-RS.AN													
42	OM-ID.GV													
43	OM-PR.AC													
44	OM-DE.CM													
45	OM-RC.IM													
46	OM-PR.DS													
47	OM-PR.IP													
48	OM-PR.PT													
49	OM-DE.DP													
50	OM-RS.CO													